

# Feedback capacity and coding for the BIBO channel with a no-repeated-ones input constraint

Oron Sabag, Haim H. Permuter and Navin Kashyap,

## Abstract

In this paper, a general binary-input binary-output (BIBO) channel is investigated in the presence of feedback and input constraints. The feedback capacity and the optimal input distribution of this setting are calculated for the case of an  $(1, \infty)$ -RLL input constraint, that is, the input sequence contains no consecutive ones. These results are obtained via explicit solution of a corresponding dynamic programming optimization problem. A simple coding scheme is designed based on the principle of posterior matching, which was introduced by Shayevitz and Feder for memoryless channels. The posterior matching scheme for our input-constrained setting is shown to achieve capacity using two new ideas: *message history*, which captures the memory embedded in the setting, and *message splitting*, which eases the analysis of the scheme. Additionally, in the special case of an S-channel, we give a very simple zero-error coding scheme that is shown to achieve capacity. For the input-constrained BSC, we show using our capacity formula that feedback increases capacity when the cross-over probability is small.

## Index Terms

Binary channels, dynamic programming, feedback capacity, posterior matching scheme, runlength-limited (RLL) constraints.

## I. INTRODUCTION

Consider the binary symmetric channel (BSC), described in Fig. 1 with  $\alpha = \beta$ , in the presence of feedback. This setting is well understood in terms of capacity,  $C = 1 - H_2(\alpha)$ , but also in terms of efficient and capacity-achieving coding schemes such as the Horstein scheme [2] and the posterior matching scheme (PMS) [3]. However, imposing constraints on the input sequence, even in the simplest cases, makes the capacity calculation challenging, since this setting is equivalent to a finite-state channel. A special case of the setting studied here is the BSC with feedback

The work of O. Sabag and H. H. Permuter was supported in part by European Research Council under the European Unions Seventh Framework Programme (FP7/2007-2013)/ERC grant agreement n°337752. All authors have also been partially supported by a Joint UGC-ISF research grant. Part of this work was presented at the 2016 Int. Conf. on Signal Processing and Communications (SPCOM 2016), Bangalore, India [1]. O. Sabag and H. H. Permuter are with the department of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Beer-Sheva, Israel (oronsa@post.bgu.ac.il, haimp@bgu.ac.il). N. Kashyap is with the department of Electrical Communication Engineering, Indian Institute of Science, Bangalore, India (nkashyap@ece.iisc.ernet.in).

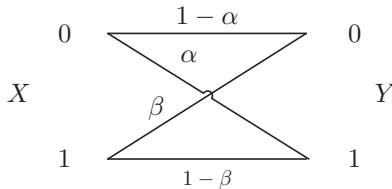


Fig. 1. BIBO channel with transition probabilities  $(\alpha, \beta)$ .

and a no-consecutive-ones input constraint (Fig. 2), that is, the channel input sequence cannot contain adjacent ones. We will show for instance, that its feedback capacity still has a simple expression:

$$C = \max_p \frac{H_2(p) + p H_2\left(\frac{\alpha(1-\alpha)}{p}\right)}{1+p} - H_2(\alpha), \quad (1)$$

and that there exists an efficient coding scheme that achieves this feedback capacity. It is also interesting to understand the role of feedback on capacity when input constraints are present, and it will be proven that in contrast to the unconstrained BSC, *feedback does increase capacity* for the input-constrained BSC.

The capacity of input-constrained memoryless channels has been extensively investigated in the literature, but still there are no computable expressions for the capacity without feedback [4]–[8]. On the other hand, in [9], it was shown that if there is a noiseless feedback link to the encoder (Fig. 2), then the feedback capacity can be formulated as a dynamic programming (DP) problem, for which there exist efficient numerical algorithms for capacity computation [10]–[17]. However, as indicated by the authors of [9], analytic expressions for the feedback capacity and the optimal input distributions are still hard to obtain and remain an open problem. In this paper, both feedback capacity and the optimal input distribution of the binary-input binary-output (BIBO) channel (Fig. 1) with a no-consecutive-ones input constraint are derived by solving the corresponding DP problem. The BIBO channel includes as special cases the BSC ( $\alpha = \beta$ ), which was studied in [9], the  $Z$ -channel ( $\alpha = 0$ ) and the  $S$ -channel ( $\beta = 0$ ).

Shannon proved that feedback does not increase the capacity of a memoryless channel [18]; following the proof of his theorem, he also claimed that “feedback does not increase the capacity for channels with memory if the internal channel state can be calculated at the encoder”. The input-constrained setting studied here can be cast as a state-dependent channel, so it fits Shannon’s description of such a channel. Therefore, we investigate the role of feedback for the special case of input-constrained BSC. In the regime  $\alpha \rightarrow 0$ , the feedback capacity from (1) is compared with a corresponding expression obtained for the capacity without feedback [19]. This comparison reveals that feedback increases capacity, at least for small enough values of  $\alpha$  for the input-constrained BSC in contrast to Shannon’s claim. However, this is not the first counterexample to Shannon’s claim; two other such counterexamples can be found in [20], [21].

In past works on channels with memory, such as [12]–[15], the optimal input distribution provided insights into the construction of simple coding schemes with zero error probability. This methodology also works for the  $S$ -channel, for which we are able to give a simple zero-error coding scheme. The coding scheme is similar to the

”repeat each bit until it gets through” policy that is optimal for a binary erasure channel with feedback. In our case, each bit is repeated with its complement until  $Y = 0$  is received, so the formed sequence is of alternating bits and satisfies the input constraint. However, a coding scheme for the general BIBO channel is challenging since  $p(y|x) > 0$ , for all  $(x, y)$ , and therefore, there is no particular pattern of outputs for which a bit can be decoded with certainty. Nonetheless, we are able to use the structure of the optimal input distribution to give a simple coding scheme, based on the principle of posterior matching as is elaborated below.

Two fundamental schemes on sequential coding for memoryless channels with feedback date back to the work of Horstein [2] for the BSC, and that of Schalkwijk and Kailath [22] for the additive white Gaussian noise (AWGN) channel. In [3], Shayevitz and Feder established the strong connection between these coding schemes by introducing a generic coding scheme, termed the *posterior matching scheme* (PMS), for all memoryless channels. This work provided a rigorous proof for the optimality of such sequential schemes, a fact that may be intuitively correct but difficult to prove. Subsequent works proved the coding optimality using different approaches [23], including an original idea by Li and El Gamal in [24] to introduce a randomizer that is available both to the encoder and the decoder. This assumption markedly simplifies the coding analysis, and it was adopted thereafter by [25] to simplify their original analysis in [3]. In our coding scheme, it is also assumed that there is a common randomizer available to all parties as a key step to the derivations of an optimal PMS for the BIBO channel.

The principle behind the PMS is to determine the channel inputs such that the optimal input distribution is simulated. For a memoryless channel, the optimal input distribution is i.i.d. so the encoder simulates the same experiment at all times. In the input-constrained setting, the input distribution is given by  $p(x_i|x_{i-1}, y^{i-1})$  (inputs are constrained with probability 1), so the conditioning injects new information on which the encoder should depend. The first element in the conditioning,  $y^{i-1}$ , can be viewed as a time-sharing (not i.i.d.) since both the encoder and the decoder know this tuple. Indeed, it is shown that they don’t need to track the entire tuple  $y^{t-1}$ , but a recursive quantization of it on a directed graph. The second element,  $x_{i-1}$ , is a new element in the PMS since it is only available to the encoder, and it is handled by introducing a new idea called *message history* for each message. The analysis of the scheme is simplified using *message splitting*, which results in homogenous Markov chain instead of

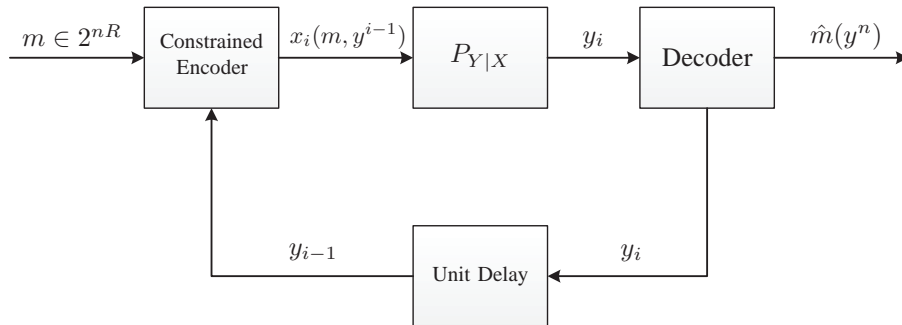


Fig. 2. System model for an input-constrained memoryless channel with noiseless feedback.

a time-dependent random process. These two ideas constitute the core of the PMS for the input-constrained setting, and it is shown that the coding scheme achieves the capacity of the general input-constrained BIBO channel.

The remainder of the paper is organized as follows: Section II presents the notations and the description of the problem. Section III states the main results of the paper. In Section IV, we provide the PMS for our input-constrained setting, while the optimality of this scheme is proven in Section V. In Section VI, we present the DP formulation of the feedback capacity together with its solution. Finally, we present our conclusion in Section VII. Proofs of some of the results from Sections III and VI are given in appendices to preserve the flow of the presentation.

## II. NOTATION AND PROBLEM DEFINITION

Random variables will be denoted by upper-case letters, such as  $X$ , while realizations or specific values will be denoted by lower-case letters, e.g.,  $x$ . Calligraphic letters, e.g.,  $\mathcal{X}$ , will denote the alphabets of the random variables. Let  $X^n$  denote the  $n$ -tuple  $(X_1, \dots, X_n)$  and let  $x^n$  denote the realization vectors of  $n$  elements, i.e.,  $x^n = (x_1, x_2, \dots, x_n)$ . For any scalar  $\alpha \in [0, 1]$ ,  $\bar{\alpha}$  stands for  $\bar{\alpha} = 1 - \alpha$ . Let  $H_2(\alpha)$  denote the binary entropy for the scalar  $\alpha \in [0, 1]$ , i.e.,  $H_2(\alpha) = -\alpha \log_2 \alpha - \bar{\alpha} \log_2 \bar{\alpha}$ .

The communication setting (Fig. 2) consists of a message  $M$  that is drawn uniformly from the set  $\{1, \dots, 2^{nR}\}$  and made available to the encoder. At time  $i$ , the encoder produces a binary output,  $x_i \in \{0, 1\}$ , as a function of  $m$ , and the output samples  $y^{i-1}$ . The sequence of encoder outputs,  $x_1 x_2 x_3 \dots$ , must satisfy the  $(1, \infty)$ -RLL input constraint, i.e., no consecutive ones are allowed. The transmission is over the BIBO channel (Fig. 1) that is characterized by two transition probabilities,  $p(Y = 1|X = 0) = \alpha$  and  $p(Y = 0|X = 1) = \beta$ , where  $\alpha$  and  $\beta$  are scalars from  $[0, 1]$ . The channel is memoryless, i.e.,  $p(y_i|x^i, y^{i-1}) = p(y_i|x_i)$  for all  $i$ .

**Definition 1.** A  $(n, 2^{nR}, (1, \infty))$  code for an input-constrained channel with feedback is defined by a set of encoding functions:

$$f_i : \{1, \dots, 2^{nR}\} \times \mathcal{Y}^{i-1} \rightarrow \mathcal{X}, \quad i = 1, \dots, n,$$

satisfying  $f_i(m, y^{i-1}) = 0$  if  $f_{i-1}(m, y^{i-2}) = 1$  (the mapping  $f_1(\cdot)$  is not constrained), for all  $(m, y^{i-1})$ , and by a decoding function  $\Psi : \mathcal{Y}^n \rightarrow \{1, \dots, 2^{nR}\}$ .

The *average probability of error* for a code is defined as  $P_e^{(n)} = \Pr(M \neq \Psi(Y^n))$ . A rate  $R$  is said to be  $(1, \infty)$ -*achievable* if there exists a sequence of  $(n, 2^{nR}, (1, \infty))$  codes such that  $\lim_{n \rightarrow \infty} P_e^{(n)} = 0$ . The *capacity*,  $C^{\text{fb}}(\alpha, \beta)$  is defined as the supremum over all  $(1, \infty)$ -achievable rates.

The transition probabilities can be restricted to  $\alpha + \beta \leq 1$ , a fact that is justified by:

**Lemma 1.** *The capacity of binary channels satisfies  $C(\alpha, \beta) = C(1 - \alpha, 1 - \beta)$ , for all  $\alpha, \beta$ .*

*Proof:* For a channel with parameters  $(\alpha, \beta)$ , apply an invertible mapping  $\tilde{Y} = Y \oplus 1$  on channel outputs so that the capacity remains the same but the parameters are changed to  $(1 - \alpha, 1 - \beta)$ . ■

The proof of the lemma is valid even when the inputs are constrained and there is feedback to the encoder.

### III. MAIN RESULTS

In this section, we present our main results concerning the feedback capacity of the BIBO channel, and thereafter, we show that feedback increases capacity for the BSC. The optimal PMS for the BIBO channel is not included in this section and appears in Section IV.

#### A. Feedback capacity

The general expression for the feedback capacity is given by the following theorem

**Theorem 1** (BIBO capacity). *The feedback capacity of the input-constrained BIBO channel is*

$$C^{\text{fb}}(\alpha, \beta) = \max_{z_L \leq z \leq z_U} \frac{H_2(\alpha \bar{z} + \bar{\beta} z) + (\alpha \bar{z} + \bar{\beta} z) H_2\left(\frac{\alpha \bar{\beta}}{\alpha \bar{z} + \bar{\beta} z}\right) - (\bar{z} + \bar{\beta} z) H_2(\alpha) - (z + \alpha \bar{z}) H_2(\beta)}{1 + \alpha \bar{z} + \bar{\beta} z}, \quad (2)$$

where  $\alpha + \beta \leq 1$ ,  $z_L = \frac{\sqrt{\alpha}}{\sqrt{\alpha} + \sqrt{\beta}}$  and  $z_U = \frac{\sqrt{\alpha}}{\sqrt{\alpha} + \sqrt{\beta}}$ .

The feedback capacity can also be expressed by:

$$C^{\text{fb}}(\alpha, \beta) = \log\left(\frac{1 - p_{\alpha, \beta}}{p_{\alpha, \beta} - \alpha \bar{\beta}}\right) + \beta \frac{H_2(\alpha)}{1 - \alpha - \beta} - \bar{\alpha} \frac{H_2(\beta)}{1 - \alpha - \beta}, \quad (3)$$

where  $p_{\alpha, \beta}$  is the unique solution of

$$(1 - \alpha \bar{\beta})[H_2(\alpha) - H_2(\beta)] + (\bar{\beta} - \alpha)[2 \log(1 - p) - \log(p - \alpha \bar{\beta})(1 + \alpha \bar{\beta}) + \alpha \bar{\beta} \log \alpha \bar{\beta}] = 0. \quad (4)$$

The proof of (2) in Theorem 1 appears in Section VI and relies on the formulation of feedback capacity as a DP problem. From the solution of the DP, we only obtain that the maximization in (2) is over  $z \in [0, 1]$ , but this can be strengthened using the following result:

**Lemma 2.** Define  $R_{\alpha, \beta}(z) = \frac{H_2(\alpha \bar{z} + \bar{\beta} z) + (\alpha \bar{z} + \bar{\beta} z) H_2\left(\frac{\alpha \bar{\beta}}{\alpha \bar{z} + \bar{\beta} z}\right) - (\bar{z} + \bar{\beta} z) H_2(\alpha) - (z + \alpha \bar{z}) H_2(\beta)}{1 + \alpha \bar{z} + \bar{\beta} z}$  with  $0 \leq z \leq 1$ . The argument that achieves the maximum of  $R_{\alpha, \beta}(z)$  lies within  $[z_L, z_U]$ , for all  $\alpha + \beta \leq 1$ . Additionally, for the BSC ( $\alpha = \beta$ ), the maximum is attained when the argument is at  $[z_L, 0.5]$ .

The proof of Lemma 2 appears in Appendix A. The alternative capacity expression (3) is obtained by taking the derivative of (2) and substituting the resulting relation into the capacity expression (2). Note that the LHS of (4) is a decreasing function, and hence, efficient methods can be applied to calculate (3).

**Remark 1.** The feedback capacity can also be calculated using upper and lower bounds from [26], instead of the DP approach that is taken in this paper.

Theorem 1 provides the capacity of three special cases: the BSC, the S-channel and the Z-channel. Their feedback capacities are calculated by substituting their corresponding parameters in Theorem 1.

**Corollary 1** (BSC capacity). *The feedback capacity of the input-constrained BSC ( $\alpha = \beta$ ) is*

$$C^{\text{BSC}}(\alpha) = \max_{\sqrt{\alpha \bar{\alpha}} \leq p \leq 0.5} \frac{H_2(p) + p H_2\left(\frac{\alpha \bar{\alpha}}{p}\right)}{1 + p} - H_2(\alpha), \quad (5)$$

where  $\alpha \leq 0.5$ . An alternative capacity expression is

$$C^{\text{BSC}}(\alpha) = \log \left( \frac{1 - p_\alpha}{p_\alpha - \alpha \bar{\alpha}} \right) - H_2(\alpha), \quad (6)$$

where  $p_\alpha$  is the unique solution of  $(\alpha \bar{\alpha})^{\alpha \bar{\alpha}} (1 - p)^2 = (p - \alpha \bar{\alpha})^{1 + \alpha \bar{\alpha}}$ .

By operational considerations, the feedback capacity in Theorem 1 serves as an upper bound for the non-feedback setting, which is still an open problem. For the BSC, it will be shown further in Theorem 2 that feedback increases capacity, at least for small values of  $\alpha$ , so this upper bound is not tight.

**Corollary 2** (S-channel capacity). *The feedback capacity of the input-constrained S-channel ( $\beta = 0$ ) is*

$$\begin{aligned} C^{\text{S}}(\alpha) &= \max_{\sqrt{\alpha \bar{\alpha}} \leq p \leq 1} \frac{H_2(p) + p H_2\left(\frac{\alpha}{p}\right) - H_2(\alpha)}{1 + p} \\ &= \max_{\sqrt{\alpha \bar{\alpha}} \leq p \leq 1} \bar{\alpha} \frac{H_2\left(\frac{1-p}{1-\alpha}\right)}{1 + p} \end{aligned} \quad (7)$$

The capacity can also be expressed by:

$$C^{\text{S}}(\alpha) = \log \left( \frac{1 - p_\alpha}{p_\alpha - \alpha} \right), \quad (8)$$

where  $p_\alpha$  is the unique solution of  $(1 - p)^2 = (p - \alpha)^{1 + \alpha \bar{\alpha}}$ .

The second capacity expression in (7) reveals a simple coding scheme with zero error probability. The coding scheme operates in two stages:

- 1) The set of messages is bijectively mapped into longer binary data streams with a fraction of ones close to  $z$  for some fixed  $z \in (0, 1)$ . This invertible mapping can be implemented, for instance, using the enumerative source coding technique [27, Example 2].
- 2) Each bit in the data stream is sent error-free by the encoder using the following procedure:

**Coding for S-channel:** Transmit a bit to the channel; as long as  $Y = 1$ , keep transmitting the NOT of the previous channel input. When  $Y = 0$  is received, the parity of consecutive ones reveals the bit that was transmitted.

The achieved rate can be measured as the average number of information bits divided by the average number of channel uses in one procedure. The average number of channel uses until  $Y = 0$  is:

$$\begin{aligned} \bar{z} \bar{\alpha} \sum_{k=1}^{\infty} (2k - 1) \alpha^{k-1} + z \bar{\alpha} \sum_{k=1}^{\infty} 2k \alpha^{k-1} &= -\bar{z} + \bar{\alpha} \sum_{k=1}^{\infty} 2k \alpha^{k-1} \\ &= \frac{1 + p}{1 - \alpha}, \end{aligned} \quad (9)$$

where  $p = z + \alpha \bar{z}$ . The average number of information bits per procedure is  $H_2(z) = H_2\left(\frac{1-p}{1-\alpha}\right)$ , and dividing this quantity by (9), we conclude that the scheme achieves capacity.

**Corollary 3** (Z-channel capacity). *The feedback capacity of the input-constrained Z-channel ( $\alpha = 0$ ) is*

$$C^{\text{Z}}(\beta) = \max_{0 \leq p \leq \beta} \frac{H_2(p) - \frac{p}{1-\beta} H_2(\beta)}{1 + p}$$

$$= -\log(1 - p_\beta), \quad (10)$$

where  $p_\beta$  is the unique solution of the quadratic equation  $(1 - p)^2 = p \cdot 2^{\frac{H_2(\beta)}{1-\beta}}$ .

The feedback capacities of the input-constrained S and Z channels are different due to the asymmetry imposed by the input constraint (Fig. 3). Note that for most values of the channel parameters, the capacity of the S-channel exceeds that of the Z-channel; intuitively, the decoder can gain more information when observing two consecutive ones in the channel output because it knows that there is one error in this transmission pair.

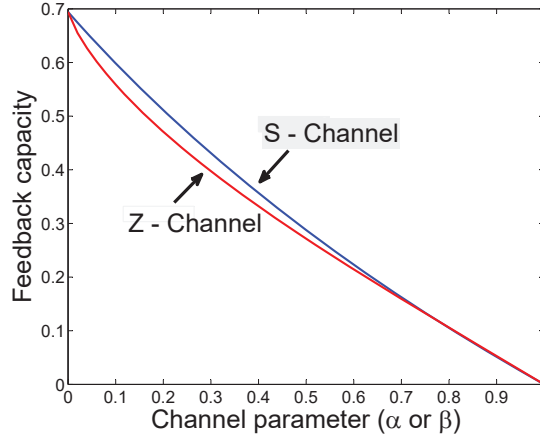


Fig. 3. Comparison between the capacities of the constrained Z- and S- channels.

### B. Feedback increases capacity

In this section, we show that feedback increases capacity for the input-constrained BSC. This provides a counterexample to a claim made by Shannon in [18].

**Theorem 2.** *Feedback increases capacity for the  $(1, \infty)$ -RLL input-constrained BSC, for all values of  $\alpha$  in some neighborhood around 0.*

As discussed in Section I, this gives a counterexample to a claim of Shannon's from [18]. A subsequent work [28] related to the conference version of our paper [29] used a novel technique to calculate upper bounds on the non-feedback capacity of the input-constrained BSC. The upper bound in [28] is a tighter upper bound than our feedback capacity, which shows that feedback increases capacity not only for small values of  $\alpha$ , but actually for all  $\alpha$ .

In order to show Theorem 2, we provide the asymptotic expressions of the input-constrained BSC with and without feedback.

**Theorem 3** (BSC asymptotic). *The feedback capacity of the input-constrained BSC is:*

$$C^{\text{BSC}}(\alpha) = \log \lambda + \frac{2 - \lambda}{3 - \lambda} \alpha \log \alpha + \left( \frac{\log(2 - \lambda) - (2 - \lambda)}{3 - \lambda} \right) \alpha + O(\alpha^2 \log^2 \alpha), \quad (11)$$

where  $\lambda$  is the golden ratio  $\left(\lambda = \frac{1+\sqrt{5}}{2}\right)$ .

The derivation of Theorem 3 is more involved than standard Taylor series expansion about  $\alpha = 0$ , since the second-order term of (11) is  $O(\alpha \log \alpha)$ . The proof of Theorem 3 appears in Appendix B.

The asymptotic of the input-constrained BSC without feedback is given by the following expression:

**Theorem 4.** [19, Example 4.1] *The non-feedback capacity of the  $(1, \infty)$ -RLL input-constrained BSC is:*

$$C^{\text{NF}}(\alpha) = \log \lambda + \frac{2\lambda + 2}{4\lambda + 3} \alpha \log \alpha + O(\alpha). \quad (12)$$

Now, it is easy to prove Theorem 2:

*Proof of Theorem 2:* The coefficients of the term  $\alpha \log \alpha$  in (11) and (12) satisfy  $\frac{2\lambda+2}{4\lambda+3} > \frac{2-\lambda}{3-\lambda}$ . Therefore, there exists  $\alpha^* > 0$  such that  $C^{\text{BSC}}(\alpha) - C^{\text{NF}}(\alpha) > 0$ , for all  $\alpha < \alpha^*$ . ■

#### IV. CAPACITY-ACHIEVING CODING SCHEME

In this section, we present the optimal input distribution in Theorem 6, and then we proceed to the main contribution of this section, the PMS for the input-constrained BIBO. The strong connection between the optimal input distribution is elaborated after Theorem 6.

##### A. Optimal input distribution

The following theorem gives the optimization problem that needs to be solved when calculating the feedback capacity of our setting.

**Theorem 5** ([14], Theorem 3). *The capacity of an  $(1, \infty)$ -RLL input-constrained memoryless channel with feedback can be written as:*

$$C^{\text{fb}} = \sup \liminf_{N \rightarrow \infty} \frac{1}{N} \sum_{t=1}^N I(X_t; Y_t | Y^{t-1}), \quad (13)$$

where the supremum is taken with respect to  $\{p(x_t | x_{t-1}, y^{t-1}) : p(X_t = 1 | X_{t-1} = 1, Y^{t-1} = y^{t-1}) = 0\}_{t \geq 1}$ .

The input at time  $t$  depends on the previous channel input,  $x_{t-1}$ , and the output samples  $y^{t-1}$ . The description of such an input distribution is difficult since the conditioning contains a time-increasing domain,  $\mathcal{Y}^{t-1}$ . The DP formulation essence is to replace the conditioning on  $y^{t-1}$  with  $p(X_{t-1} = 0 | Y^{t-1} = y^{t-1})$ , which is a sufficient statistic of the outputs tuple. Furthermore, the DP solution in Section VI reveals that the *optimal input distribution* can be described even with a simpler notion called a  $Q$ -graph, which is suitable for scenarios where the DP state,  $p(X_{t-1} = 0 | Y^{t-1} = y^{t-1})$ , takes a finite number of values.

**Definition 2.** For an output alphabet,  $\mathcal{Y}$ , a  $Q$ -graph is a directed, connected and labelled graph. Additionally, each node should have  $|\mathcal{Y}|$  outgoing edges, with distinct labels.

See the defined  $Q$ -graph in Fig. 4 that will be used to describe the optimal input distribution. Given some initial node on the  $Q$ -graph and an output sequence of arbitrary length, a unique node can be calculated by walking



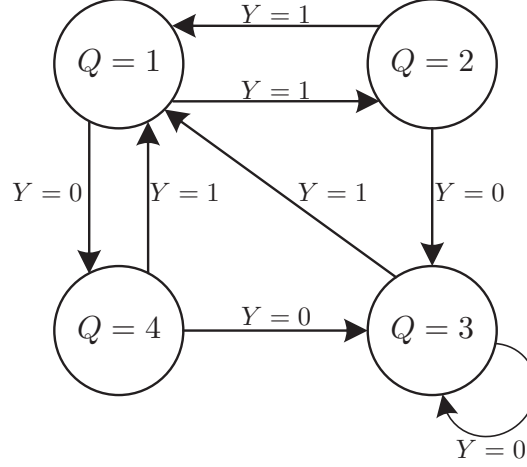


Fig. 4. The  $Q$ -graph that characterizes the optimal input distribution.

along the graph according to the labelled edges until the sequence ends. The mapping that is induced by this graph is denoted by  $\Phi_t : \mathcal{Y}^{t-1} \rightarrow \mathcal{Q}$ , or equivalently, with a function  $g$  such that  $\Phi_t(y^t) = g(\Phi_{t-1}(y^{t-1}), y_t)$ . The importance of the  $Q$ -graph for our scheme is that the encoder and decoder need only track the value  $\Phi_{t-1}(y^{t-1})$ , instead of the entire output sequence  $y^{t-1}$ .

For the description of the optimal input distribution, define

$$z_2^{\alpha, \beta} = \arg \max_{0 \leq z \leq 1} \frac{H_2(\alpha \bar{z} + \bar{\beta} z) + (\alpha \bar{z} + \bar{\beta} z) H_2\left(\frac{\alpha \bar{\beta}}{\alpha \bar{z} + \bar{\beta} z}\right) - (\bar{z} + \bar{\beta} z) H_2(\alpha) - (z + \alpha \bar{z}) H_2(\beta)}{1 + \alpha \bar{z} + \bar{\beta} z}, \quad (14)$$

with the following subsequent quantities:

$$\begin{aligned} z_1^{\alpha, \beta} &\triangleq \frac{\alpha \bar{z}_2^{\alpha, \beta}}{\alpha \bar{z}_2^{\alpha, \beta} + \bar{\beta} z_2^{\alpha, \beta}} \\ z_3^{\alpha, \beta} &\triangleq \frac{\bar{\alpha} \bar{z}_2^{\alpha, \beta}}{\bar{\alpha} \bar{z}_2^{\alpha, \beta} + \beta z_2^{\alpha, \beta}} \\ z_4^{\alpha, \beta} &\triangleq \frac{\bar{\alpha} \bar{\beta} z_2^{\alpha, \beta}}{\bar{\alpha} \bar{\beta} z_2^{\alpha, \beta} + \alpha \beta z_2^{\alpha, \beta}}. \end{aligned} \quad (15)$$

It can be shown that  $z_1^{\alpha, \beta} \leq z_2^{\alpha, \beta} \leq z_3^{\alpha, \beta} \leq z_4^{\alpha, \beta}$  for all  $\alpha + \beta \leq 1$ . For instance, the relation  $z_1 \leq z_2$  (superscripts  $(\alpha, \beta)$  are omitted) can be simplified to  $(\bar{\beta} - \alpha)z_2^2 + 2\alpha z_2 - \alpha \geq 0$ . Now, the polynomial  $(\bar{\beta} - \alpha)x^2 + 2\alpha x - \alpha$  has two roots, one is negative and the other is at  $x = z_L$ . Since the polynomial is convex,  $(\bar{\beta} - \alpha)z_2^2 + 2\alpha z_2 - \alpha \geq 0$  is equivalent to  $z_2 \geq z_L$  which is proved in Lemma 2. The other relations follow from similar arguments.

Define the conditional distributions

$$P_{X|X^-, Q=1}^* = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$P_{X|X^-, Q=2}^* = P_{X|X^-, Q=1}^*$$

$$\begin{aligned}
P_{X|X^-,Q=3}^* &= \begin{bmatrix} 1 - \frac{z_2^{\alpha,\beta}}{z_3^{\alpha,\beta}} & \frac{z_2^{\alpha,\beta}}{z_3^{\alpha,\beta}} \\ 1 & 0 \end{bmatrix} \\
P_{X|X^-,Q=4}^* &= \begin{bmatrix} 1 - \frac{z_2^{\alpha,\beta}}{z_4^{\alpha,\beta}} & \frac{z_2^{\alpha,\beta}}{z_4^{\alpha,\beta}} \\ 1 & 0 \end{bmatrix},
\end{aligned} \tag{16}$$

in which  $X^-$  corresponds to rows and  $X$  to columns.

The optimal input distribution and alternative capacity expression are given in the following theorem:

**Theorem 6** (Optimal input distribution). *The input distribution  $p(X_i = x|X_{i-1} = x^-, Y^{i-1} = y^{i-1}) = P_{X|X^-,Q}^*(x|x^-, \Phi_{i-1}(y^{i-1}))$ , defined in (16) and Fig. 4, is capacity-achieving. Moreover, the random process  $\{(X_i, Q_i)\}_{i \geq 1}$ , induced by  $P_{X|X^-,Q}^*$  is a first-order Markov chain. Denoting the stationary distribution of this Markov chain as  $\pi_{X^-,Q}(x^-, q)$ , the feedback capacity can be expressed as  $I(X; Y|Q)$ , where the joint distribution is  $\pi(q, x, y) = \sum_{x^-} p(y|x)P^*(x|x^-, q)\pi(x^-, q)$ .*

The simplified structure of the optimal input distribution in Theorem 6 is the basis for our coding scheme construction. The scheme uses the joint probability  $P_{Y|X}P_{X|X^-,Q}^*\pi_{X^-,Q}$ , that is induced by the optimal input distribution  $P_{X|X^-,Q}^*$ . Here,  $X$  and  $X^-$  should be viewed as the channel inputs during the current and previous time instances, respectively, and  $Q$  is the value of the node on the  $Q$ -graph prior to the transmission of  $X$ . Furthermore, the scheme analysis uses the first-order Markov property to show that  $I(X; Y|Q)$  is achievable. The proof of Theorem 6 is presented at the end of Section VI.

### B. The coding scheme

The main element of the PMS is the posterior distribution of each message interval given the channel outputs. The posterior distribution will be represented by a length of an interval in the unit interval, where initial lengths are equal for all message intervals since the decoder has no information on the message at the beginning. The lengths of the intervals are updated throughout the transmission based on the outputs that are made available to the decoder (and to the encoder from the feedback). The encoder's rule is to refine the decoder's knowledge about the correct message such that the corresponding message interval length will increase to 1 and the decoder can successfully declare its estimation for the correct message.

For the input-constrained setting, we use message splitting (to be defined later), which prevents the length of the correct message interval from increasing to 1. However, it is still possible to show that, with high probability, the length of the correct message interval increases above some constant. Therefore, the PMS output is a list of messages whose lengths are above the constant. We refer to the PMS as Part I of our coding scheme, and its output is a list of "suspected" correct messages. To determine which message in this list is the correct message, a zero-rate code, based on the method of types, will be introduced as Part II.

The PMS (Part I) is described by the following building-blocks:

- 1) Message intervals

- 2) Initialization of message intervals
- 3) Random shift
- 4) Message splitting and transmission
- 5) Update of message intervals
- 6) Decoder decision on message list

### *Preliminaries*

A message  $M$  is selected uniformly from the set of messages  $\mathcal{M} = \{1, 2, \dots, 2^{nR}\}^1$  and is transmitted using the PMS scheme. Our aim is to show that the probability that the decoded list of messages does not contain the correct message vanishes as  $n$  grows.

It is assumed that the encoder and the decoder share some common randomness:

- an initial state  $Q_0 \sim \pi_Q$ , where  $\pi_Q$  denotes the marginal distribution on  $Q$  of  $\pi_{X^-, Q}$ ;
- i.i.d. sequence  $(U_i)_{i=1}^n$ , where  $U_i \sim \text{Unif}[0, 1]$ .

Additionally, we assume that encoder has a local randomizer, an i.i.d. sequence, denoted by  $(V_i)_{i=1}^n$ , where  $V_i \sim \text{Unif}[0, 1]$ . The assumption of shared randomness simplifies our analysis and was also adopted in [24] and [25]. By standard averaging arguments, the shared knowledge can be “de-randomized” in the sense that there exists a deterministic instantiation of  $Q_0$  and  $(U_i)_{i=1}^n, (V_i)_{i=1}^n$  for which the probability of error analysis will remain valid.

### *Message intervals*

Message intervals are data structures central to the operation of the PMS scheme. At each time instant  $i \geq 1$ , the decoder and the encoder can compute a common set,  $\mathcal{J}_{i-1}$ , consisting of message intervals. Each message interval,  $J \in \mathcal{J}_{i-1}$ , can be identified by its left end-point  $t_{i-1}(J)$  and its length  $s_{i-1}(J)$ , so that  $J = [t_{i-1}(J), t_{i-1}(J) + s_{i-1}(J))$ . The message intervals form a partition of  $[0, 1)$  into disjoint sub-intervals of varying lengths, each of which is associated with a message.

At the beginning of the transmission, a one-to-one mapping,  $\tau_0 : \mathcal{J}_0 \leftrightarrow \mathcal{M}$  associates each message with a distinct message interval. Along the transmission, the set of message intervals may be increased so the initial mapping  $\tau_0$  is not valid anymore. However, there exists a surjective mapping  $\tau_i : \mathcal{J}_i \rightarrow \mathcal{J}_{i-1}$ , for all  $i \geq 1$ , and therefore, a message interval can be translated into a message from  $\mathcal{M}$  using the function composition  $\mu_i \triangleq \tau_0 \circ \dots \circ \tau_i$ .

The length of  $J \in \mathcal{J}_{i-1}$  equals the posterior probability that  $J$  is the message interval, given  $(y^{i-1}, u^{i-1})$ , i.e.,

$$s_{i-1}(J, y^{i-1}, u^{i-1}) = \Pr(J_{i-1} = J \mid Y^{i-1} = y^{i-1}, U^{i-1} = u^{i-1}), \quad (17)$$

where  $J_{i-1}$  is the random variable denoting the correct message interval at time  $i - 1$ . Additionally, each  $J \in \mathcal{J}_{i-1}$  has a “history bit”, denoted by  $x_{i-1}^-(J)$ , which is the bit that the encoder would have transmitted at time  $i - 1$  if it

<sup>1</sup>To simplify the description,  $2^{nR}$  is assumed to be an integer; we may otherwise take the number of messages to be  $\lceil 2^{nR} \rceil$ .

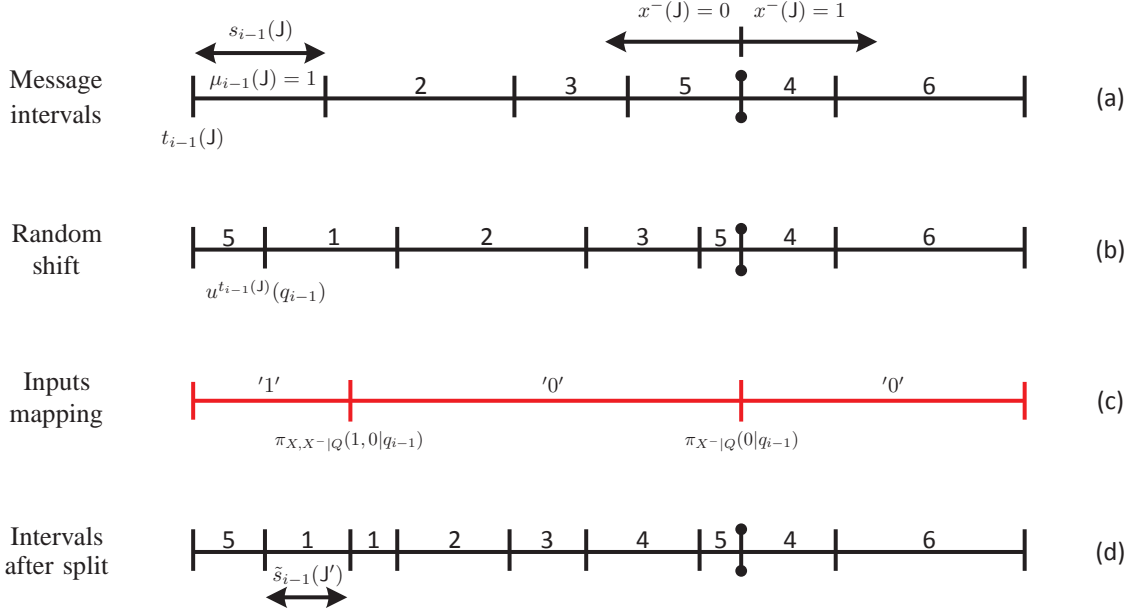


Fig. 5. Illustration of the coding scheme. The lengths of the message intervals are determined by their posterior probabilities, and the message intervals are positioned in ascending order based on their history. Each message interval with  $x^-(J) = 0$  is modulo-shifted by adding the randomizer  $u_i(q_{i-1})$  and its new left-end is  $u^{t_{i-1}(J)}(q_{i-1})$ . The inputs mapping is fixed for a given  $q_{i-1}$ , and message intervals that cross its boundary points are split into two intervals. In this example, the message interval, denoted by 1, is split into two parts at the boundary point  $\pi_{X,X-Q}(1,0|q_{i-1})$  and the interval 5 is split at  $\pi_{X-Q}(0|q_{i-1})$ .

were actually true that  $J_{i-1} = J$ . For each message interval, define the set of all messages intervals in  $\mathcal{J}_{i-1}$  with identical history bit, and such that their message is smaller than  $\mu_{i-1}(J)$ :

$$\mathcal{W}_{i-1}(J) = \{J' : \mu_{i-1}(J') < \mu_{i-1}(J), x_{i-1}^-(J') = x_{i-1}^-(J)\},$$

which give rise to the left-end positions at time  $i-1$ :

$$t_{i-1}(J) = \mathbb{1}_{x_{i-1}^-(J)=1} \pi_{X-Q}(0|q_{i-1}) + \sum_{J' \in \mathcal{W}_{i-1}(J)} s_{i-1}(J').$$

The positioning rule implies that the unit interval consists of different-length message intervals, where intervals with  $x^-(J) = 0$  are positioned on the left part of the unit interval, while all other intervals are on the right part (Fig. 5(a)).

In summary, a message interval  $J \in \mathcal{J}_{i-1}$  stores four pieces of data:  $\mu_{i-1}(J)$ ,  $s_{i-1}(J)$ ,  $t_{i-1}(J)$  and  $x_{i-1}^-(J)$ . As we will see, these are computable at both the encoder and the decoder from their common knowledge at time  $i$ .

#### Initialization of message intervals

At time  $i = 0$ , each message  $m \in \mathcal{M}$  is mapped to the interval  $J = [(m-1)2^{-nR}, m2^{-nR})$ , so the mapping  $\tau_0$  is made clear. The lengths of all message intervals is identical,  $s_0(J) = 2^{-nR}$ , and their history bit,  $x_0^-(J)$ , is

determined by:

$$x_0^-(J) = \begin{cases} 0 & \text{if } t_0(J) \in [0, \pi(X^- = 0|Q_0 = q_0)) \\ 1 & \text{if } t_0(J) \in [\pi(X^- = 0|Q_0 = q_0), 1). \end{cases} \quad (18)$$

We assume that the messages fit the intervals in (18) perfectly, which can be justified by performing message splitting (defined below) at time  $i = 0$ . The random variable corresponding to the message interval at the beginning is  $J_0 = \tau_0^{-1}(M)$ , where  $\tau_0^{-1}$  is the inverse of  $\tau_0$ .

#### Random shift

The random shift operation results in a circular shift of all message intervals with  $x_{i-1}^-(J) = 0$ , that is, all message intervals that fall in  $[0, \pi(X^- = 0|Q = q_{i-1}))$ . Recall that  $u_i$  is the randomization available to the encoder and the decoder, and then the shift operation is performed by adding  $u_i(q_{i-1}) \triangleq u_i \cdot \pi_{X^-|Q}(0|q_{i-1})$  to each message interval and taking  $\text{mod } \pi_{X^-|Q}(0|q_{i-1})$  (See Fig. 5(b)). The left-end position after the random shift of  $J$  is denoted by the function  $u_i^{t_{i-1}(J)}(q_{i-1}) \triangleq t_{i-1}(J) + u_i(q_{i-1}) \text{ mod } \pi_{X^-|Q}(0|q_{i-1})$ .

#### Message splitting and transmission

The channel inputs mapping, denoted by  $x : \mathcal{Q} \times [0, 1) \rightarrow \mathcal{X}$ , is given by

$$x(q, t) = \begin{cases} 1 & \text{if } t \in [0, \pi(X = 1, X^- = 0|Q = q)) \\ 0 & \text{if } t \in [\pi(X = 1, X^- = 0|Q = q), 1), \end{cases} \quad (19)$$

as is illustrated in Fig. 5(c). Ideally, each point in a message interval is mapped to the same input when applying  $x(\cdot)$ . However, if the left and right ends of a message interval are mapped to different inputs it is not clear which symbol to transmit<sup>2</sup>. Specifically, if a message interval contains one of the boundary points:

$$\pi(X = 1, X^- = 0|Q = q_{i-1}) \quad (20)$$

$$\pi(X^- = 0|Q = q_{i-1}), \quad (21)$$

then it is *split* into two message intervals. For example, in Fig. 5(d), the message labelled with 1 has been split by (20) and the message 5 was split by (21).

The case that the boundary point (20) falls in a message interval  $J$  is now elaborated, while the details for the other boundary point are omitted. If  $J$  is split at the point (20), then two intervals,  $J'$  and  $J''$ , are formed as follows:

$$J' = [u_i^{t_{i-1}(J)}(q_{i-1}), \pi(X = 1, X^- = 0|Q = q_{i-1}))$$

$$J'' = [\pi(X = 1, X^- = 0|Q = q_{i-1}), u_i^{t_{i-1}(J)}(q_{i-1}) + s_{i-1}(J)).$$

<sup>2</sup>Message intervals can be split into two intervals at most, since the transmission is terminated at any time instance that a message interval exceeds  $s_{i-1}(J) \geq S_{min} \triangleq \min_{x, x^-, q: \pi(X=x, X^-=x^-|Q=q)>0} \pi(X=x, X^-=x^-|Q=q)$ .

At this stage, all message intervals, after the split has occurred, are identified with  $\tilde{t}_{i-1}(J)$  and  $\tilde{s}_{i-1}(J)$ , that correspond to the left-end and the length of each message interval, respectively. The new message intervals  $J'$  and  $J''$  are associated with  $J$  through the surjective mapping,  $\tau_i : \mathcal{J}_i \rightarrow \mathcal{J}_{i-1}$ , that returns  $\tau_i(J') = \tau_i(J'') = J$ . Also,  $\tau_i(J) = J$  for all the message intervals that are not split.

The message interval length after the split,  $\tilde{s}_{i-1}(J, y^{i-1}, u^i)$ , can be expressed as:

$$\tilde{s}_{i-1}(J, y^{i-1}, u^i) = \Pr(J_i = J | y^{i-1}, u^i). \quad (22)$$

It can be noted from the series of equations (20)-(22) that  $\tilde{s}_{i-1}(\cdot)$  is a function of  $q_{i-1}, u_i^{t_{i-1}(J)}(q_{i-1}), s_{i-1}(\tau_i(J))$ , so we may sometimes write it as  $\tilde{s}_{i-1}(q_{i-1}, u_i^{t_{i-1}(J)}(q_{i-1}), s_{i-1}(\tau_i(J)), x^-(J))$ .

Finally, we define the message interval at time  $i$ ,  $J_i$ , that determines the channel input at time  $i$ . In case that the message interval  $J_{i-1}$  is not split, then  $J_i = J_{i-1}$ . If  $J_{i-1}$  is split into two parts, say  $J'$  and  $J''$ , then the local randomizer,  $v_i$ , is used to generate a uniform distribution on  $s_{i-1}(J)$ . Then, define  $J_i = J'$  if  $v_i \cdot s_{i-1}(J) < \pi(X = 1, X^- = 0 | Q = q_{i-1}) - u_i^{t_{i-1}(J)}(q_{i-1})$ , and otherwise it is the other message interval  $J_i = J''$ . It is now easy to define the transmitted symbol at time  $i$  as a function of  $\tilde{t}_{i-1}(J_i)$  and  $q_{i-1}$  as  $x_i = x(q_{i-1}, \tilde{t}_{i-1}(J_i))$ .

#### Update of message intervals

The recursive update of the message interval lengths is given by:

**Lemma 3.** *The length of message interval  $J \in \mathcal{J}_i$  can be calculated as follows:*

$$s_i(J) = \tilde{s}_{i-1}(q_{i-1}, u_i^{t_{i-1}(J)}(q_{i-1}), s_{i-1}(\tau_i(J)), x_{i-1}^-(J)) \frac{p(Y = y_i | X = x(q_{i-1}, \tilde{t}_{i-1}(J)))}{\pi(Y = y_i | Q = q_{i-1})}.$$

The purpose of this lemma is two-fold: on the one hand, it provides a simple method to compute the message interval lengths from the set of message intervals at the previous time. The other role of this lemma is to emphasize that  $s_i(J)$  can be computed from  $(q_{i-1}, u_i^{t_{i-1}(J)}(q_{i-1}), s_{i-1}(\tau_i(J)), x_{i-1}^-(J), y_i)$ .

*Proof of Lemma 3:* Recall that the lengths are defined as:

$$\begin{aligned} s_i(J) &= p(J_i = J | Y^i = y^i, U^i = u^i) \\ &= \frac{p(Y_i = y_i, J_i = J | Y^{i-1} = y^{i-1}, U^i = u^i)}{p(Y_i = y_i | Y^{i-1} = y^{i-1}, U^i = u^i)} \\ &= \frac{\tilde{s}_{i-1}(q_{i-1}, u_i^{t_{i-1}(J)}(q_{i-1}), s_{i-1}(\tau_i(J))) p(Y_i = y_i | J_i = J, Y^{i-1} = y^{i-1}, U^i = u^i)}{p(Y_i = y_i | Y^{i-1} = y^{i-1}, U^i = u^i)} \\ &= \frac{\tilde{s}_{i-1}(q_{i-1}, u_i^{t_{i-1}(J)}(q_{i-1}), s_{i-1}(\tau_i(J))) p(Y = y_i | X = x(q_{i-1}, \tilde{t}_{i-1}(J)))}{p(Y_i = y_i | Y^{i-1} = y^{i-1}, U^i = u^i)}. \end{aligned}$$

For the denominator, consider

$$\begin{aligned} &p(Y_i = y_i | Y^{i-1} = y^{i-1}, U^i = u^i) \\ &= \sum_{J \in \tilde{\mathcal{J}}_{i-1}} P(Y_i = y_i, J_i = J | Y^{i-1} = y^{i-1}, U^i = u^i) \end{aligned}$$

$$\begin{aligned}
&= \sum_{J \in \tilde{\mathcal{J}}_{i-1}} \tilde{s}_{i-1}(J, y^{i-1}, u^i) p(Y_i = y_i | J_i = J, Y^{i-1} = y^{i-1}, U^i = u^i) \\
&\stackrel{(a)}{=} p(X = 1, X^- = 0 | Q = q_{i-1}) P(Y_i = y_i | X_i = 1) + (1 - p(X = 1, X^- = 0 | Q = q_{i-1})) p(Y_i = y_i | X_i = 0) \\
&= \pi(Y = y_i | Q = q_{i-1}),
\end{aligned}$$

where (a) follows by the definition of inputs mapping  $x(\cdot)$  in (19).  $\blacksquare$

#### Decoder decision on message list

Let  $T$  be the first time that there exists  $J$  such that  $s_T(J) \geq \xi^* \triangleq \max\{\xi, S_{\min}\}$ , where  $\xi$  is defined in the proof and  $S_{\min} = \min_{x, x^-, q: \pi(X=x, X^-=x^- | Q=q) > 0} \pi(X=x, X^-=x^- | Q=q)$ . The decoder then declares a list of messages  $\hat{\mathcal{M}} := \{\mu_T(J) \in \mathcal{M} : s_T(J) \geq \xi^*\}$ . The size of the decoded list is bounded by  $|\hat{\mathcal{M}}| \leq \lfloor \frac{1}{\xi^*} \rfloor$ , and can be described with  $k \triangleq \lceil \log \lfloor \frac{1}{\xi^*} \rfloor \rceil$  bits.

The analysis of the PMS part (Part I) is encapsulated in the following fundamental theorem, which is proved in Section V:

**Theorem 7.** *For all  $\epsilon > 0$ , if  $R < I(X; Y | Q)$ , there exists  $N_0(\epsilon)$  and  $\xi > 0$  such that  $\Pr(S_n(J_n) < \xi) \leq \epsilon$  for all  $n \geq N_0(\epsilon)$ .*

**Part II:** The message list generated by Part I is the input for Part II, a complementary scheme to determine the correct message within  $\hat{\mathcal{M}}$ . The rate of this part can be made to go to zero, since it only has to distinguish between a bounded number of messages in  $\mathcal{M}$ . Each message in  $\hat{\mathcal{M}}$  is represented with  $k$  bits,  $b_1 b_2 \dots b_k$ , to be transmitted consecutively.

**Encoder:** Given a stream of  $k$  bits,  $b_1, \dots, b_k$ , the encoder transmits bit by bit using a repetition code (of length  $L/2$ ) at odd times and '0' at even times.

**Decoder:** Based on the  $L/2$  outputs (at the odd times), the decoder declares  $\hat{b}_L = 0$  if the output sequence lies in the typical set  $\mathcal{T}_\epsilon^{(n)}(P_{Y|X=0})$ , and declares  $\hat{b}_L = 1$  otherwise.

The analysis of Part II is made for transmission of one bit:

**Lemma 4.** *For all  $\epsilon > 0$ , if  $C^{\text{fb}}(\alpha, \beta) \neq 0$ , there exists  $L^*(\epsilon)$  such that  $\Pr(\hat{b}_L \neq b) \leq \epsilon$ , for all  $L \geq L^*(\epsilon)$ .*

*Proof:* The decoding rule is a standard typicality argument based on the fact that if capacity is non-zero then

$$D(P_{Y|X=0} || P_{Y|X=1}) \neq 0,$$

so there exists a sequence  $\epsilon'(n) > 0$  such that  $\mathcal{T}_{\epsilon'(n)}^{(n)}(P_{Y|X=0}) \cap \mathcal{T}_{\epsilon'(n)}^{(n)}(P_{Y|X=1}) = \emptyset$  and both typical sets are nonempty.

Without loss of generality, assume that the transmitted bit is  $X = 0$ , and thus, the output sequence (at odd times) is i.i.d.  $\sim P_{Y|X=0}$ . By standard arguments, it can be shown that the probability of the output sequence to be in  $\mathcal{T}_{\epsilon'}^{(n)}(P_{Y|X=0})$  (for some  $0 < \epsilon' < \epsilon'(n)$ ) grows exponentially, while the probability of the output sequence to be

in  $\mathcal{T}_e^{(n)}(P_{Y|X=1})$  decays exponentially. Therefore, there exists some  $L^* \in \mathbb{N}$  such that  $\Pr(\hat{b}_{L^*} \neq b)$  is small, as desired. ■

Finally, the optimality of the overall coding scheme that combines Part I and Part II can be shown:

**Theorem 8.** *For an input-constrained BC, any rate  $R < C^{\text{fb}}(\alpha, \beta)$  is achievable using the PMS and part II.*

*Proof of Theorem 8:* To design a block-code with probability of error  $\epsilon$ , we compute  $N_0(\frac{\epsilon}{2})$  from Theorem 7 and  $L^*(\frac{\epsilon}{2k})$  from Lemma 4. Now, we construct a code of length  $n = N_0(\frac{\epsilon}{2}) + kL^*(\frac{\epsilon}{2k})$ , where the PMS is applied at the first  $N_0(\frac{\epsilon}{2})$  times and in the remaining  $kL^*(\frac{\epsilon}{2k})$  times, the coding in Part II is applied. Consider the probability of error,

$$\begin{aligned} P_e^{(n)} &= \Pr(M \neq \hat{M}_n) \\ &\leq \Pr(M \notin \hat{M}_{N_0(\frac{\epsilon}{2})}) + k \cdot \Pr(b_i \neq \hat{b}_i | M \in \hat{M}_{N_0(\frac{\epsilon}{2})}) \\ &\leq \frac{\epsilon}{2} + k \cdot \frac{\epsilon}{2k} \\ &= \epsilon, \end{aligned}$$

where the second inequality follows from Theorem 7 and Lemma 4. ■

## V. PMS ANALYSIS

We prove Theorem 7 that includes that the probability of error in Part I (PMS) can be made arbitrarily small.

### A. Preliminaries

Define for  $\rho \in [0, 1)$ ,

$$\phi_{q^-, x, q}(\rho) \triangleq \left( \frac{p(Y = y | X = x)}{p(Y = y | Q = q^-)} \right)^{-\rho}, \quad (23)$$

where  $y$  is the unique solution for the equation  $q = g(q^-, y)$ . We also use  $\phi_{(x, q)_{i-1}^i}(\rho)$  as a shorthand for  $\phi_{q_{i-1}, x_i, q_i}(\rho)$ . Throughout the analysis, it is assumed that  $p(y|x) > 0$ , otherwise define  $\phi_{q^-, x, q}(\rho) = 0$  for all  $(x, y)$  with  $p(y|x) = 0$  and the derivation can be repeated.

Define also:

$$\psi_{x^-, q^-, x, q}^s(\rho) \triangleq \mathbb{E}[(S_i(J_i)/S_{i-1}(J_{i-1}))^{-\rho} | J_{i-1} = J, S_{i-1}(J) = s, X_{i-1}(J) = x^-, Q_{i-1} = q^-, X_i = x, Q_i = q].$$

Indeed, there should also be a time index, but it will be shown that the distribution does not depend on time. To simplify notation, we omit the dependence on the message intervals, i.e.,

$$\psi_{x^-, q^-, x, q}^s(\rho) \triangleq \mathbb{E}[(S_i/S_{i-1})^{-\rho} | S_{i-1} = s, X_{i-1} = x^-, Q_{i-1} = q^-, X_i = x, Q_i = q].$$



## B. Analysis

The following lemma comprises the core of our PMS analysis:

**Lemma 5.** *For all  $\delta > 0$ , there exists  $s^*(\delta)$  such that*

$$\psi_{x^-,q^-,x,q}^s(\rho) \leq \phi_{q^-,x,q}(\rho)2^\delta,$$

for all  $s \leq s^*(\delta)$ ,  $0 \leq \rho < 1$ , and all  $x^-, q^-, x, q$ .

*Proof of Lemma 5:* In this proof we show that  $\psi_{x^-,q^-,x,q}^s(\rho)$  can be made arbitrarily close to  $\phi_{q^-,x,q}(\rho)$  if we take  $s$  to be small enough. Recall that we restrict transmission to be as long as  $s \leq S_{\min} = \min_{x,x^-,q;\pi(X=x,X^-=x^-|Q=q)>0} \pi(X=x, X^-=x^-|Q=q)$ . From Lemma 3, we have

$$\begin{aligned} \psi_{x^-,q^-,x,q}^s(\rho) &= \mathbb{E}[S_i^{-\rho}/S_{i-1}^{-\rho} | S_{i-1} = s, X_{i-1} = x^-, Q_{i-1} = q^-, X_i = x, Q_i = q] \\ &= \left( \frac{p(Y=y|X=x)}{\pi(Y=y|Q=q^-)} \right)^{-\rho} \mathbb{E}[\tilde{S}_{i-1}^{-\rho}/S_{i-1}^{-\rho} | S_{i-1} = s, X_{i-1} = x^-, Q_{i-1} = q^-, X_i = x, Q_i = q] \\ &= \phi_{q^-,x,q}(\rho) \mathbb{E}[\tilde{S}_{i-1}^{-\rho}/S_{i-1}^{-\rho} | S_{i-1} = s, X_{i-1} = x^-, Q_{i-1} = q^-, X_i = x, Q_i = q]. \end{aligned} \quad (24)$$

Therefore, our interest is to show an upper bound on the expected value above. The simpler case is when  $X_{i-1} = 1$ , since there is no split (that is,  $s_{i-1}(\cdot) = \tilde{s}_{i-1}(\cdot)$ ) and then  $\psi_{1,q^-,x,q}^s(\rho) = \phi_{q^-,x,q}(\rho)$ .

For the other case  $X_{i-1} = 0$ , consider the density function of the randomizers:

$$\begin{aligned} &f_{U_i^{t_{i-1}(J)}(q^-), V_i | X_i, Q_i, X_{i-1}, Q_{i-1}, S_{i-1}}(u, v | x, q, 0, q^-, s) \\ &= \frac{p(X_i = x, Q_i = q | X_{i-1} = 0, Q_{i-1} = q^-, U_i^{t_{i-1}(J)}(q^-) = u, V_i = v, S_{i-1} = s)}{p(X_i = x, Q_i = q | X_{i-1} = 0, Q_{i-1} = q^-, S_{i-1} = s)} f_{U_i^{t_{i-1}(J)}(q^-), V_i}(u, v) \\ &\stackrel{(a)}{=} \frac{p(X_i = x | X_{i-1} = 0, Q_{i-1} = q^-, U_i^{t_{i-1}(J)}(q^-) = u, V_i = v, S_{i-1} = s)}{p(X_i = x | X_{i-1} = 0, Q_{i-1} = q^-, S_{i-1} = s^-)} f_{U_i(q^-), V_i}(u, v) \\ &\stackrel{(b)}{=} \frac{p(X_i = x | X_{i-1} = 0, Q_{i-1} = q^-, U_i^{t_{i-1}(J)}(q^-) = u, V_i = v, S_{i-1} = s)}{p(X_i = x | X_{i-1} = 0, Q_{i-1} = q^-)} f_{U_i(q^-), V_i}(u, v) \\ &\stackrel{(c)}{=} \frac{p(X_i = x | X_{i-1} = 0, Q_{i-1} = q^-, U_i^{t_{i-1}(J)}(q^-) = u, V_i = v, S_{i-1} = s)}{P_{x,0,q^-}} f_{U_i, V_i} \left( \frac{u}{\pi_{X^-|Q}(0|q^-)}, v \right), \end{aligned} \quad (25)$$

where (a) follows from the Markov chain  $Q_i - (X_i, Q_{i-1}) - (S_{i-1}, X_{i-1}, U_i, V_i)$  and the fact that  $U_i^{t_{i-1}(J)}(q^-)$  is distributed uniformly on  $[0, \pi(X^- = 0 | Q = q^-)]$  for any value  $t_{i-1}(J)$ , (b) follows from the Markov chain  $X_i - (X_{i-1}, Q_{i-1}) - S_{i-1}$  and (c) is due to replacement of the r.v.  $U_i(q^-)$  with  $U_i$ , and the notation  $P_{x,0,q^-} \triangleq p(X_i = x, X_{i-1} = 0 | Q_{i-1} = q^-)$ . The Markov chain  $Q_i - (X_i, Q_{i-1}) - (S_{i-1}, X_{i-1}, U_i, V_i)$  follows from the fact that  $Q_i$  is a function of  $(Y_i, Q_{i-1})$  and the memoryless property. The second Markov chain  $X_i - (X_{i-1}, Q_{i-1}) - S_{i-1}$  is shown in two steps: first, if  $X_{i-1} = 1$ , then  $X_i = 0$ . For the other case,  $X_{i-1} = 0$ , note that  $\tilde{t}_{i-1}(J)$  (given  $(X_{i-1} = 0, Q_{i-1} = q_{i-1})$ ) is distributed uniformly on  $[0, \pi(X^- = 0 | Q = q_{i-1})]$  and  $X_i$  is a function of  $\tilde{t}_{i-1}(J)$  and  $q_{i-1}$ .

Note that the numerator of (25) is an indicator function of the event that the point  $(u + sv) \bmod \pi(X^- = 0 | Q = q^-)$  is mapped to  $X_i = x$ . Also, recall the density definition  $f_{U,V}(u, v) = 1$  for all  $(u, v) \in [0, 1] \times [0, 1]$ .

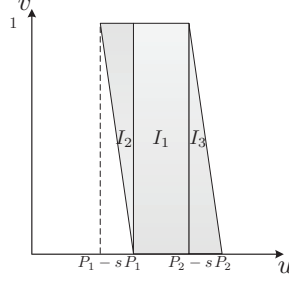


Fig. 6. Illustration of the intervals in (27). We use  $P_1 \triangleq \pi(X = 1, X^- = 0|Q = q^-)$   $P_2 \triangleq \pi(X^- = 0|Q = q^-)$ . The colored area corresponds to values of  $u$  and  $v$  for which  $p(X_i = 0|X_{i-1} = 0, Q_{i-1} = q^-, U_i^{t_{i-1}^{(J)}}(q^-) = u, V_i = v, S_{i-1} = s) = 1$ .

We begin with the calculation of the expected value in (24) for the case  $X_i = 0$ :

$$\begin{aligned}
 & \mathbb{E}[\tilde{S}_{i-1}^{-\rho}/S_{i-1}^{-\rho}|S_{i-1} = s, X_{i-1} = 0, Q_{i-1} = q^-, X_i = 0, Q_i = q] \\
 & \stackrel{(a)}{=} s^\rho \int_{[0, \pi(X^- = 0|Q = q^-)]} \int_{[0, 1]} f_{U_i(q^-), V_i|X_i, Q_i, X_{i-1}, Q_{i-1}, S_{i-1}}(u, v|0, q, 0, q^-, s^-) \tilde{s}(q^-, u, s^-, 0)^{-\rho} dv du \\
 & \stackrel{(b)}{=} \frac{s^\rho}{P_{0,0,q^-}} \int_{I_1 \cup I_2 \cup I_3} \int_{[0, 1]} p(X_i = x|X_{i-1} = 0, Q_{i-1} = q^-, U_i^{t_{i-1}^{(J)}}(q^-) = u, V_i = v, S_{i-1} = s) \tilde{s}(q^-, u, s^-, 0)^{-\rho} dv du,
 \end{aligned} \tag{26}$$

where

- (a) follows from the notation  $\tilde{s}(q^-, u, s^-, 0)$  defined in (22) which stands for the interval length after a split, and the domain for which  $f_{U_i, V_i}(\frac{u}{\pi_{X^-|Q}(0|q^-)}, v) = 1$ ;
- (b) follows from substituting (25) and restricting the integration over  $u$ , the left-end point of the message interval after modulo-shifting, to the intervals where  $p(X_i = 0|X_{i-1} = 0, Q_{i-1} = q^-, U_i^{t_{i-1}^{(J)}}(q^-) = u, V_i = v, S_{i-1} = s) = 1$ , i.e.,

$$\begin{aligned}
 I_1 & \triangleq [\pi(X = 1, X^- = 0|Q = q^-), \pi(X^- = 0|Q = q^-) - s] \\
 I_2 & \triangleq [\pi(X = 1, X^- = 0|Q = q^-) - s, \pi(X = 1, X^- = 0|Q = q^-)] \\
 I_3 & \triangleq [\pi(X^- = 0|Q = q^-) - s, \pi(X^- = 0|Q = q^-)],
 \end{aligned} \tag{27}$$

which are illustrated in Fig. 6.

For the interval,  $I_1$ , note that  $\tilde{s}_{i-1}(\cdot) = s_{i-1}(\cdot)$  regardless of the values of  $u$  and  $v$ , so

$$\begin{aligned}
 & \frac{s^\rho}{P_{0,0,q^-}} \int_{I_1} \int_{[0, 1]} p(X_i = 0|X_{i-1} = 0, Q_{i-1} = q^-, U_i^{t_{i-1}^{(J)}}(q^-) = u, V_i = v, S_{i-1} = s) \tilde{s}(q^-, u, s^-, 0)^{-\rho} dv du \\
 & = \frac{1}{P_{0,0,q^-}} |I_1| \\
 & = \frac{P_{0,0,q^-} - s}{P_{0,0,q^-}}.
 \end{aligned}$$

For the interval  $I_2$ , note from Fig. 6 that  $p(X_i = 0|X_{i-1} = 0, Q_{i-1} = q^-, U_i^{t_{i-1}^{(J)}}(q^-) = u, V_i = v, S_{i-1} =$

$s) = 1$  only when  $v \in \left[ \frac{-u+P_{0,0,q^-}}{s}, 1 \right]$  (See Fig. 6), therefore,

$$\begin{aligned}
& \frac{s^\rho}{P_{0,0,q^-}} \int_{I_2} \int_{[0,1]} p(X_i = 0 | X_{i-1} = 0, Q_{i-1} = q^-, U_i^{t_{i-1}^{(j)}}(q^-) = u, V_i = v, S_{i-1} = s) \tilde{s}(q^-, u, s^-, 0)^{-\rho} dv du \\
& \stackrel{(a)}{=} \frac{s^\rho}{P_{0,0,q^-}} \frac{1}{s} \int_{I_2} (u - P_{0,0,q^-} + s) (u - P_{0,0,q^-} + s)^{-\rho} du \\
& = \frac{s^\rho}{P_{0,0,q^-}} \frac{1}{s} \int_{[0,s]} u^{-\rho+1} du \\
& = \frac{1}{P_{0,0,q^-}} \frac{s}{(-\rho+2)},
\end{aligned}$$

where (a) follows from  $\tilde{s}(u, x^-, q^-, x) = u - P_{0,0,q^-} + s$ . The calculation for the third interval,  $I_3$ , is similar to that for  $I_2$  and results in the same value of integration.

To conclude, we showed that

$$\begin{aligned}
\psi_{0,q^-,x,q}^s(\rho) &= \phi_{q^-,x,q}(\rho) \left[ \frac{\pi(X = x, X^- = 0 | Q = q^-) - s}{\pi(X = x, X^- = 0 | Q = q^-)} + 2 \frac{1}{\pi(X = x, X^- = 0 | Q = q^-)} \frac{s}{(-\rho+2)} \right] \\
&\triangleq \phi_{q^-,x,q}(\rho) 2^{\delta_{q^-,x}(s)}
\end{aligned}$$

for  $\rho \in [0, 1)$ . The last step is to define  $\delta(s) \triangleq \max_{q^-,x} \delta_{q^-,x}(s)$ , which goes to zero when  $s \rightarrow 0$ . Now, it is clear that  $\psi_{x^-,q^-,x,q}^s(\rho) \leq \phi_{q^-,x,q}(\rho) 2^{\delta(s)}$  for all  $(x^-, q^-, x, q)$ ,  $0 \leq \rho < 1$  and  $s \leq S_{\min}$ , as required.  $\blacksquare$

*Proof of Theorem 7:* Recall from Lemma 5 that for all  $\delta > 0$ , there exists  $s^*(\delta)$ , such that for all  $s \leq s^*(\delta)$

$$\psi_{x^-,q^-,x,q}^s(\rho) \leq \phi_{q^-,x,q}(\rho) 2^\delta. \quad (28)$$

We will utilize (28) to provide an upper bound on  $\mathbb{E}[\Lambda(S_n(J_n))]$ , where  $\Lambda(s) = s^{-\rho}$  is a decreasing function for some  $\rho \geq 0$ . The upper bound will be shown to vanish with  $n$ , and applying the Markov with the decreasing function  $\Lambda(\cdot)$  concludes that the probability of error vanishes as well.

The following notation is used in the forthcoming derivations: let  $\Delta_i = (X_i, Q_i, S_i)$  and let  $(X, Q)_i^j$  stand for  $(X_i^j, Q_i^j)$  when  $i < j$ . Finally, let  $S_n$  denotes  $S_n(J_n)$ , and consider the following chain of inequalities,

$$\begin{aligned}
& \mathbb{E}_{\Delta_n}[\Lambda(S_n)] \\
& \stackrel{(a)}{=} \mathbb{E}_{\Delta_{n-1}}[\Lambda(S_{n-1}) \mathbb{E}_{\Delta_n | \Delta_{n-1}}[\Lambda(S_n/S_{n-1}) | \Delta_{n-1}]] \\
& = \mathbb{E}_{\Delta_{n-1}}[\Lambda(S_{n-1}) \mathbb{E}_{(X_n, Q_n) | \Delta_{n-1}}[\mathbb{E}_{S_n | (X_n, Q_n), \Delta_{n-1}}[\Lambda(S_n/S_{n-1}) | (X_n, Q_n), \Delta_{n-1}]]] \\
& \stackrel{(b)}{\leq} \mathbb{E}_{\Delta_{n-1}}[\Lambda(S_{n-1}) \mathbb{E}_{(X_n, Q_n) | \Delta_{n-1}}[\phi_{(X,Q)_{n-1}^n}(\rho)]] 2^\delta \\
& = \mathbb{E}_{(X,Q)_{n-1}^n}[\phi_{(X,Q)_{n-1}^n}(\rho) \mathbb{E}_{S_{n-1} | (X,Q)_{n-1}^n}[\Lambda(S_{n-1}) | (X, Q)_{n-1}^n]] 2^\delta \\
& \stackrel{(a)}{=} \mathbb{E}_{(X,Q)_{n-1}^n}[\phi_{(X,Q)_{n-1}^n}(\rho) \mathbb{E}_{\Delta_{n-2} | (X,Q)_{n-1}^n}[\Lambda(S_{n-2}) \mathbb{E}_{S_{n-1} | (X,Q)_{n-1}^n, \Delta_{n-2}}[\Lambda(S_{n-1}/S_{n-2}) | (X, Q)_{n-1}^n, \Delta_{n-2}]]] 2^\delta \\
& \stackrel{(c)}{=} \mathbb{E}_{(X,Q)_{n-1}^n}[\phi_{(X,Q)_{n-1}^n}(\rho) \mathbb{E}_{\Delta_{n-2} | (X,Q)_{n-1}^n}[\Lambda(S_{n-2}) \mathbb{E}_{S_{n-1} | (X_{n-1}, Q_{n-1}), \Delta_{n-2}}[\Lambda(S_{n-1}/S_{n-2}) | (X_{n-1}, Q_{n-1}), \Delta_{n-2}]]] 2^\delta \\
& \stackrel{(b)}{\leq} \mathbb{E}_{(X,Q)_{n-1}^n}[\phi_{(X,Q)_{n-1}^n}(\rho) \mathbb{E}_{\Delta_{n-2} | (X,Q)_{n-1}^n}[\Lambda(S_{n-2}) \phi_{(X,Q)_{n-2}^{n-1}}(\rho)]] 2^{2\delta} \\
& = \mathbb{E}_{(X,Q)_{n-2}^{n-1}}[\phi_{(X,Q)_{n-1}^n}(\rho) \phi_{(X,Q)_{n-2}^{n-1}}(\rho) \mathbb{E}_{S_{n-2} | (X,Q)_{n-2}^{n-1}}[\Lambda(S_{n-2}) | (X, Q)_{n-2}^{n-1}]] 2^{2\delta}
\end{aligned}$$

$$\begin{aligned}
&\stackrel{(d)}{\leq} \mathbb{E}_{(X,Q)_1^n} \left[ \prod_{i=1}^n \phi_{(X,Q)_{i-1}}(\rho) \mathbb{E}_{S_0|(X,Q)_1^n} [\Lambda(S_0)|(X,Q)_1^n] \right] 2^{n\delta} \\
&= 2^{nR\rho} 2^{n\delta} \mathbb{E}_{(X,Q)_1^n} \left[ \prod_{i=1}^n \phi_{(X,Q)_{i-1}}(\rho) \right],
\end{aligned}$$

where:

- (a) follows from the law of total expectation;
- (b) follows from (28) since  $\psi_{X_{n-1}, Q_{n-1}, X_n, Q_n}^{S_{n-1}}(\rho) = \mathbb{E}_{S_n|(X_n, Q_n), \Delta_{n-1}} [\Lambda(S_n/S_{n-1})|(X_n, Q_n), \Delta_{n-1}]$ ;
- (c) follows from the Markov chain  $S_i - (\Delta_{i-1}, (X_i, Q_i)) - (X, Q)_{i+1}^n$  for all  $i$ , and specifically, for  $i = n-1$ . This Markov chain follows from the same argument used in Lemma 5 for the Markov chain  $X_{i+1} - (X_i, Q_i) - S_i$
- (d) follows from applying the above steps  $n-2$  times;

The expectation above can be decomposed into non-typical and typical sequences with respect to the Markov distribution  $p(q, x|q^-, x^-) = \sum_y \mathbb{1}\{q = g(q^-, y)\} p(y|x) P_{X|X^-, Q}^*(x|x^-, q^-)$ . With some abuse of notation, since  $q^-$  and  $q$  determine a unique  $y$  such that  $q = g(q^-, y)$ , we refer to  $\phi_{(X,Q)_{i-1}}(\rho)$  as  $\phi_{Q_{i-1}, X_i, Y_i}(\rho)$ . Consider

$$\begin{aligned}
\mathbb{E}_{\Delta_n} [g(S_n)] &\stackrel{(a)}{\leq} 2^{n(R\rho+\delta)} \left[ \epsilon_n \left[ \max_{q^-, x, y} \phi_{q^-, x, y}(\rho) \right]^n + \prod_{q^-, x, y} \phi_{q^-, x, y}(\rho)^{n\pi(q^-, x, y) + \kappa_n} \right] \\
&= 2^{n(R\rho+\delta+K\rho)} \epsilon_n + 2^{n(R\rho+\delta)} \prod_{q^-, x, y} 2^{(n\pi(q^-, x, y) + \kappa_n) \log \phi_{q^-, x, y}(\rho)} \\
&= 2^{n(R\rho+\delta+K\rho)} \epsilon_n + 2^{n(R\rho+\delta)} 2^{-\rho \sum_{q^-, x, y} (n\pi(q^-, x, y) + \kappa_n) \log \left( \frac{p(y|x)}{\pi(y|q^-)} \right)} \\
&\stackrel{(b)}{\leq} 2^{n(R\rho+\delta+K\rho)} \epsilon_n + 2^{-n\rho(I(X;Y|Q) - R - \frac{\delta}{\rho} + \frac{\kappa'_n}{n})}, \tag{29}
\end{aligned}$$

where (a) follows from separating the contributions made to the expected value by non-typical and typical sequences: we let  $\epsilon_n$  denote the probability that a sequence is not in the typical set,  $K$  stands for  $\max_{q, x, y} \log \left( \frac{\pi(y|q)}{p(y|x)} \right)$  and, finally,  $\kappa_n$  denotes the maximal correcting factor of the empirical distribution from  $\pi(q^-, x, y)$ . Item (b) follows from the notation  $\kappa'_n \triangleq \kappa_n |\mathcal{Q}| |\mathcal{X}| |\mathcal{Y}| K$ . Now, since  $\epsilon_n$  decreases exponentially with  $n$ , there exists a choice,  $(\rho^*, \delta^*)$  such that  $2^{n(R\rho+\delta+K\rho)} \epsilon_n$  is arbitrary small, while  $R$  can be made arbitrarily close to  $I(X;Y|Q)$ .

Finally, the main result can be derived with  $\delta^*$  and  $\rho^*$

$$\begin{aligned}
\Pr(S_n(J_n) \leq s^*(\delta^*)) &\stackrel{(a)}{=} \Pr(\Lambda(S_n(J_n)) \geq \Lambda(s^*(\delta^*))) \\
&\stackrel{(b)}{\leq} \frac{\mathbb{E}[\Lambda(S_n)]}{\Lambda(s^*(\delta^*))} \\
&\stackrel{(c)}{\rightarrow} 0, \tag{30}
\end{aligned}$$

where (a) follows from the fact that  $\Lambda(\cdot)$  is a decreasing function, (b) follows from Markov's inequality and (c) follows from (29). ■

## VI. DP FORMULATION AND SOLUTION

This section covers the formulation of feedback capacity as DP and its solution. The solution of the DP problem implies almost immediately the derivations of feedback capacity and optimal input distribution, which were stated

earlier as separate results in Theorems 1 and 6 (which are proved at the end of this section). We begin with presenting the family of DP problems termed infinite-horizon with average reward.

#### A. Average reward DP

Each DP is defined by the tuple  $(\mathcal{Z}, \mathcal{U}, \mathcal{W}, F, P_Z, P_w, g)$ . We consider a discrete-time dynamical system evolving according to:

$$z_t = F(z_{t-1}, u_t, w_t), \quad t = 1, 2, \dots \quad (31)$$

Each state,  $z_t$ , takes values in a Borel space  $\mathcal{Z}$ , each action,  $u_t$ , takes values in a compact subset  $\mathcal{U}$  of a Borel space, and each disturbance,  $w_t$ , takes values in a measurable space  $\mathcal{W}$ . The initial state,  $z_0$ , is drawn from the distribution  $P_Z$ , and the disturbance,  $w_t$ , is drawn from  $P_w(\cdot|z_{t-1}, u_t)$ . The history,  $h_t = (z_0, w_1, \dots, w_{t-1})$ , summarizes all the information available to the controller at time  $t$ . The controller at time  $t$  chooses the action,  $u_t$ , by a function  $\mu_t$  that maps histories to actions, i.e.,  $u_t = \mu_t(h_t)$ . The collection of these functions is called a policy and is denoted as  $\pi = \{\mu_1, \mu_2, \dots\}$ . Note that given a policy,  $\pi$ , and the history,  $h_t$ , one can compute the actions vector,  $u^t$ , and the states of the system,  $z_1, z_2, \dots, z_{t-1}$ .

Our objective is to maximize the average reward given a bounded reward function  $r : \mathcal{Z} \times \mathcal{U} \rightarrow \mathbb{R}$ . The average reward for a given policy  $\pi$  is given by:

$$\rho_\pi = \liminf_{N \rightarrow \infty} \frac{1}{N} \mathbb{E}_\pi \left[ \sum_{t=1}^N r(Z_{t-1}, \mu_t(h_t)) \right],$$

where the subscript indicates that actions  $u_t$  are subject to the policy  $\pi$ . The optimal average reward is defined as

$$\rho = \sup_{\pi} \rho_\pi.$$

Having defined the DP problem, we are ready to show the formulation of feedback capacity as DP.

#### B. Formulation of capacity as DP

The state of the DP,  $z_{t-1}$ , is defined as the conditioned probability vector  $\beta_{t-1}(x_{t-1}) \triangleq p(x_{t-1}|y^{t-1})$ . The action space,  $\mathcal{U}$ , is the set of stochastic matrices,  $p(x_t|x_{t-1})$ , such that  $p(x_t = 1|x_{t-1} = 1) = 0$ . For a given policy and an initial state, the encoder at time  $t-1$  can calculate the state,  $\beta_{t-1}$ , since the tuple  $y^{t-1}$  is available from the feedback. The disturbance is taken to be the channel output,  $w_t = y_t$ , and the reward gained at time  $t-1$  is chosen as  $I(Y_t; X_t|y^{t-1})$ . These definitions imply that the optimal reward of this DP is equal to the feedback capacity given in Theorem 5.

It can also be shown that the DP states satisfy the following recursive relation,

$$\begin{aligned} \beta_t(x_t) &= p(x_t|y^t) \\ &= \frac{\sum_{x_{t-1}} \beta_{t-1}(x_{t-1}) u_t(x_t, x_{t-1}) p(y_t|x_t)}{\sum_{x_t, x_{t-1}} \beta_{t-1}(x_{t-1}) u_t(x_t, x_{t-1}) p(y_t|x_t)}, \end{aligned} \quad (32)$$

where  $u_t(x_t, x_{t-1})$  corresponds to  $p(x_t|x_{t-1}, y^{t-1})$  with an implicit dependence on the tuple  $y^{i-1}$ . In [14], this formulation was shown to satisfy the Markov nature required in DP problems and it was also shown that the

TABLE I  
THE CONDITIONAL DISTRIBUTION  $p(y_t, x_t, x_{t-1}|z_{t-1}, u_t)$

| $x_{t-1}$ | $x_t$ | $y_t = 0$                      | $y_t = 1$                     |
|-----------|-------|--------------------------------|-------------------------------|
| 0         | 0     | $\bar{\alpha}z_{t-1}u_t(1, 1)$ | $\alpha z_{t-1}u_t(1, 1)$     |
| 0         | 1     | $\beta z_{t-1}u_t(1, 2)$       | $\bar{\beta}z_{t-1}u_t(1, 2)$ |
| 1         | 0     | $\bar{\alpha}(1 - z_{t-1})$    | $\alpha(1 - z_{t-1})$         |

optimal average reward is exactly the capacity expression in Theorem 5. Note that this formulation is valid for any memoryless channel with our input constraint; moreover, minor variations can also yield a similar formulation with different input constraints.

### C. The DP for the BIBO channel

Here, each element in the formulation above will be calculated for the BIBO channel; the DP state at time  $t - 1$ ,  $z_{t-1}$ , is the probability vector  $[p(x_{t-1} = 0|y^{t-1}), p(x_{t-1} = 1|y^{t-1})]$ . Since the components of this vector sum to 1, the notation can be abused as  $z_{t-1} \triangleq p(x_{t-1} = 0|y^{t-1})$ , i.e., the first component will be the DP state. Each action,  $u_t$ , is a constrained  $2 \times 2$  stochastic matrix,  $p(x_t|x_{t-1})$ , of the form:

$$u_t = \begin{bmatrix} p(x_t = 0|x_{t-1} = 0) & p(x_t = 1|x_{t-1} = 0) \\ 1 & 0 \end{bmatrix}.$$

The disturbance  $w_t$  is the channel output,  $y_t$ , and thus, it can take values from  $\{0, 1\}$ .

The notation  $\delta_t \triangleq z_{t-1}p(x_t = 1|x_{t-1} = 0)$  is useful and implies the constraint  $0 \leq \delta_t \leq z_{t-1}$ , since  $u_t$ , by definition, must be a stochastic matrix. Furthermore, given  $z_{t-1}$ ,  $u_t$  can be recovered from  $\delta_t$  for all  $z_{t-1} \neq 0$ . For the case  $z_{t-1} = 0$ , we will see that  $u_t(1, 2)$  has no effect on the DP, so it can be fixed to zero. The system equation can then be calculated from (32):

$$z_t = \begin{cases} \frac{\bar{\alpha}\bar{\delta}_t}{(1-\alpha)(1-\delta_t)+\beta\delta_t} & \text{if } w_t = 0, \\ \frac{\alpha\bar{\delta}_t}{\alpha(1-\delta_t)+(1-\beta)\delta_t} & \text{if } w_t = 1. \end{cases} \quad (33)$$

The conditional distribution,  $p(x_t, x_{t-1}, y_t|z_{t-1}, u_t)$ , is described in Table I, so one can calculate the reward:

$$\begin{aligned} r(z_{t-1}, u_t) &= I(Y_t; X_t|z_{t-1}, u_t) \\ &= H_2(\bar{\alpha}\bar{\delta}_t + \beta\delta_t) - (1 - \delta_t)H_2(\alpha) - \delta_t H_2(\beta). \end{aligned}$$

Before computing the DP operator, it is convenient to define:

$$\begin{aligned} p_{\alpha, \beta}(\delta) &= \alpha\bar{\delta} + \bar{\beta}\delta \\ \arg 1_{\alpha, \beta}(\delta) &= \frac{\bar{\alpha}\bar{\delta}}{1 - p_{\alpha, \beta}(\delta)} \\ \arg 2_{\alpha, \beta}(\delta) &= \frac{\alpha\bar{\delta}}{p_{\alpha, \beta}(\delta)}, \end{aligned} \quad (34)$$

where the subscripts  $\alpha, \beta$  in (34) are omitted when it is clear from the context. The DP operator is then given by:

$$(Th_{\alpha,\beta})(z) = \max_{0 \leq \delta \leq z} H_2(p(\delta)) - (1 - \delta)H_2(\alpha) - \delta H_2(\beta) + (1 - p(\delta))h_{\alpha,\beta}(\arg 1(\delta)) + p(\delta)h_{\alpha,\beta}(\arg 2(\delta)), \quad (35)$$

for all functions  $h_{\alpha,\beta} : [0, 1] \rightarrow \mathbb{R}$ , parameterized by  $(\alpha, \beta)$ .

Now when the DP problem for the BIBO channel is well-defined, the Bellman equation which can verify the optimality of rewards, can be used to obtain an analytic solution. However, the Bellman equation cannot be easily solved, and therefore, numerical algorithms are required to estimate the Bellman components. The numerical study of DP problems is not within the scope of this paper, and the reader may find [12], [13] to be suitable references for learning this topic in the context of feedback capacities. Therefore, we proceed directly to the statement and the solution of the Bellman equation.

#### D. The Bellman Equation

In DP, the Bellman equation suggests a sufficient condition for average reward optimality. This equation establishes a mechanism for verifying that a given average reward is optimal. The next result encapsulates the Bellman equation:

**Theorem 9** (Theorem 6.2, [30]). *If  $\rho \in \mathbb{R}$  and a bounded function  $h : \mathcal{Z} \rightarrow \mathbb{R}$  satisfies for all  $z \in \mathcal{Z}$ :*

$$\rho + h(z) = \sup_{u \in \mathcal{U}} r(z, u) + \int P_W(dw|z, u)h(F(z, u, w)), \quad (36)$$

*then  $\rho^* = \rho$ . Furthermore, if there is a function  $\mu : \mathcal{Z} \rightarrow \mathcal{U}$ , such that  $\mu(z)$  attains the supremum for each  $z$ , then  $\rho^* = \rho_\pi$  for  $\pi = \{\mu_0, \mu_1, \dots\}$  with  $\mu_t(h_t) = \mu(z_{t-1})$  for each  $t$ .*

This result is a direct consequence of Theorem 6.2 in [30]; specifically, the triplet  $(\rho, h(\cdot), \mu(\cdot))$  is a canonical triplet by Theorem 6.2, since it satisfies (36). Now, because a canonical triplet defines for all  $N$  the  $N$ -stage optimal reward and policy under terminal cost  $h(\cdot)$ , it can be concluded that a canonical triplet also defines the optimal reward and policy in the infinite horizon regime, since in this case, the bounded terminal cost has a negligible effect.

Define the function  $R_{\alpha,\beta} : [0, 1] \rightarrow \mathbb{R}$ :

$$R_{\alpha,\beta}(z) = \frac{H_2(\alpha\bar{z} + \bar{\beta}z) + (\alpha\bar{z} + \bar{\beta}z)H_2(\frac{\alpha\bar{\beta}}{\alpha\bar{z} + \bar{\beta}z}) - (\bar{z} + \bar{\beta}z)H_2(\alpha) - (z + \alpha\bar{z})H_2(\beta)}{1 + \alpha\bar{z} + \bar{\beta}z}, \quad (37)$$

and two constants,

$$\begin{aligned} \tilde{\rho}_{\alpha,\beta} &= \max_{0 \leq z \leq 1} R_{\alpha,\beta}(z) \\ z_{\alpha,\beta}^{\text{opt}} &= \arg \max_{0 \leq z \leq 1} R_{\alpha,\beta}(z). \end{aligned} \quad (38)$$

Also, define the functions:

$$\begin{aligned} h_1^{\alpha,\beta}(z) &= H_2(p(z)) - (1 - z)H_2(\alpha) - zH_2(\beta) \\ X^{\alpha,\beta}(z) &= H_2(p(z)) - (1 - z)H_2(\alpha) - zH_2(\beta) - p(z)\tilde{\rho}_{\alpha,\beta} \end{aligned}$$

$$h_2^{\alpha,\beta}(z) = \frac{X^{\alpha,\beta}(z) + p(z)X^{\alpha,\beta}(\arg 2_{\alpha,\beta}(z))}{1 - \alpha\beta}, \quad (39)$$

for  $z \in [0, 1]$ . The concatenation of the above functions can be defined:

$$\tilde{h}_{\alpha,\beta}(z) = \begin{cases} h_1^{\alpha,\beta}(z); & \text{if } 0 \leq z \leq z_1^{\alpha,\beta} \\ h_2^{\alpha,\beta}(z); & \text{if } z_1^{\alpha,\beta} < z \leq z_2^{\alpha,\beta} \\ \tilde{\rho}_{\alpha,\beta} & \text{if } z_2^{\alpha,\beta} < z \leq 1, \end{cases}$$

where  $z_1^{\alpha,\beta}$  and  $z_2^{\alpha,\beta}$  were defined in (15). With these definitions, we are ready to state the fundamental theorem of this section.

**Theorem 10.** *The function  $\tilde{h}_{\alpha,\beta}(z)$  and the constant  $\tilde{\rho}_{\alpha,\beta}$  satisfy the Bellman equation, i.e.,*

$$\tilde{h}_{\alpha,\beta} + \tilde{\rho}_{\alpha,\beta} = T\tilde{h}_{\alpha,\beta},$$

for all  $[\alpha, \beta] \in [0, 1] \times [0, 1]$  satisfying  $\alpha + \beta \leq 1$ . Moreover, the maximum in  $T\tilde{h}_{\alpha,\beta}$  is achieved when  $\delta^*(z) = z$  for  $z \in [0, z_2^{\alpha,\beta}]$ , and  $\delta^*(z) = z_2^{\alpha,\beta}$  otherwise.

See Appendix C for the proof of Theorem 10. By Theorem 10, the feedback capacity and the optimal input distribution of the BIBO channel as stated in Theorems 1 and 6:

*Proof of Theorem 1:* By Theorem 10, the DP optimal average reward is  $\tilde{\rho}_{\alpha,\beta}$ , which is the same capacity expression from Theorem 1. ■

*Proof of Theorem 6:* In this proof, we show that the DP states under the optimal policy visit a finite set only which concludes the representation of the optimal input distribution on the  $Q$ -graph in Fig. 4. Then, it is shown that the alternative capacity expression is equal to the capacity.

Recall the optimal actions from Theorem 10:

$$\delta^*(z) = \begin{cases} z; & \text{if } 0 \leq z \leq z_2^{\alpha,\beta} \\ z_2^{\alpha,\beta}; & \text{if } z_2^{\alpha,\beta} < z \leq 1. \end{cases}$$

The DP states evolution in (33) is described with the  $\arg j_{\alpha,\beta}$  functions in (34). The set  $\mathcal{Z} \triangleq \{z_i^{\alpha,\beta}\}_{i=1}^4$ , defined in (15), is closed under the functions  $\arg j_{\alpha,\beta}(\delta)$ , that is,  $\arg j_{\alpha,\beta}(\delta^*(z_i^{\alpha,\beta})) \in \mathcal{Z}$  for all  $i, j$ . The functions  $\arg j_{\alpha,\beta}(\delta^*(z))$  (for  $j = 1, 2$ ) create a sink, meaning that there is always a positive probability for a transition to  $\mathcal{Z}$  and zero probability to leave the set, therefore, we can assume that the initial DP state is from  $\mathcal{Z}$ . To see that the evolution of the DP states can be described on a  $Q$ -graph, note that  $j = g(i, y)$  iff  $z_j^{\alpha,\beta} = \arg y_{\alpha,\beta}(\delta^*(z_i^{\alpha,\beta}))$ , for all  $i \neq j$  and  $y \in \{0, 1\}$ , and the function  $g(\cdot)$  is the one describes the transitions in the  $Q$ -graph in Fig. 4.

The following equalities verify the first-order Markov property of  $(X_i, Q_i)_{i \geq 1}$ :

$$\begin{aligned} p(x_i, q_i | x^{i-1}, q^{i-1}) &= \sum_{y_i} p(y_i, x_i, q_i | x^{i-1}, q^{i-1}) \\ &\stackrel{(a)}{=} \sum_{y_i} p(q_i | q_{i-1}, y_i) p(y_i | x_i) P_{X|X^-, Q}^*(x_i | x_{i-1}, q_{i-1}), \end{aligned} \quad (40)$$



where (a) follows from the structure of  $P_{X|X^-,Q}^*$ , the memoryless channel property and the fact that  $Q_i$  is a function of  $(Q_{i-1}, Y_i)$ .

The stationary distribution of (40) is described as follows: let  $Q$  be a random variable that takes values from  $\{1, 2, 3, 4\}$ . Define a probability vector on  $Q$ ,  $\pi_Q = [\pi(Q=1), \pi(Q=2), \pi(Q=3), \pi(Q=4)] = \left[ \frac{p}{1+p}, \frac{pq}{1+p}, \frac{1-p}{1+p}, \frac{p(1-q)}{1+p} \right]$ , where  $p = p(z_2^{\alpha,\beta})$  and  $q = \frac{\alpha(1-\alpha)}{p}$ . Also, let  $\pi_{X^-|Q}(0|i) = z_i^{\alpha,\beta}$  for  $i = 1, \dots, 4$ . Now, it can be verified that  $\pi_{X^-,Q} = \pi_{X^-|Q}\pi_Q$  is the unique stationary distribution of the Markov chain  $(X_i, Q_i)_{i \geq 1}$ .

The finiteness of the DP states visited under optimal policy implies that the feedback capacity can be written as  $\sum_{i=1}^4 \pi_Q(i) r(z_i^{\alpha,\beta}, \delta^*(z_i^{\alpha,\beta}))$ , where  $r(z_i^{\alpha,\beta}, \delta^*(z_i^{\alpha,\beta})) = I(Y; X|Q=i)$  is the optimal reward at the DP state  $z_i^{\alpha,\beta}$  and  $\pi_Q$  is defined above. ■

## VII. SUMMARY AND CONCLUDING REMARKS

The capacity of the BIBO channel with input constraints was derived using a corresponding DP problem. A by-product of the DP solution is the optimal input distribution, which can be described compactly using  $Q$ -graphs. For the S-channel, we were able to derive a capacity-achieving coding scheme with simple and intuitive analysis for the achieved rate. For the general BIBO channel, we provided a PMS which includes new elements that capture the system memory, such as, message history and message splitting. These were introduced to facilitate the proof that the PMS is indeed capacity-achieving for the general BIBO channel.

The ideas presented here for the PMS may be exploited to derive a PMS for a broader class of finite-state channels (FSC) with feedback. Specifically, a FSC is *unifilar* if the channel state is a deterministic function of the previous channel state, input and output. Though several works have proposed the PMS approach for this class, the optimality (capacity-achieving) proof remains to be solved [31], [32]. Indeed, the idea of message history that was presented in this paper can also be used for unifilar channels, since the encoder can calculate the channel state at each time. Moreover, in all unifilar channels whose feedback capacities are known, the  $Q$ -graph is an exact representation of their optimal input distributions; thus, there is a Markov chain in the process of  $(q_i, s_i)$ . In such scenarios, it can be useful to use our message splitting idea to render this Markov chain time-homogenous.

## APPENDIX A

### PROOF OF LEMMA 2

In this appendix, we first show that the argument that achieves the maximum of

$$R_{\alpha,\beta}(z) = \frac{H_2(\alpha\bar{z} + \bar{\beta}z) + (\alpha\bar{z} + \bar{\beta}z)H_2\left(\frac{\alpha\bar{\beta}}{\alpha\bar{z} + \bar{\beta}z}\right) - (\bar{z} + \bar{\beta}z)H_2(\alpha) - (z + \alpha\bar{z})H_2(\beta)}{1 + \alpha\bar{z} + \bar{\beta}z}$$

lies within  $[z_L, z_U] = \left[ \frac{\sqrt{\alpha}}{\sqrt{\alpha} + \sqrt{\beta}}, \frac{\sqrt{\alpha}}{\sqrt{\alpha} + \sqrt{\beta}} \right]$ .

Let  $p(z) = \alpha\bar{z} + \bar{\beta}z$  and denote by  $p'$  the derivative of  $p(z)$ . After some simplifications, the derivative equals:

$$\begin{aligned} \frac{d}{dz} R(z) &= \frac{1}{(1 + p(z))^2} \left\{ (1 - \alpha\bar{\beta})(H_2(\alpha) - H_2(\beta)) + (\bar{\beta} - \alpha) [2 \log(1 - p(z)) - \log(p(z) - \alpha\bar{\beta})(1 + \alpha\bar{\beta}) + \alpha\bar{\beta} \log \alpha\bar{\beta}] \right\} \end{aligned}$$

The above derivative equals zero when the function

$$f_{\alpha,\beta}(z) \triangleq (1 - \alpha\bar{\beta})[H_2(\alpha) - H_2(\beta)] + (\bar{\beta} - \alpha)[2\log(1 - p(z)) - \log(p(z) - \alpha\bar{\beta})(1 + \alpha\bar{\beta}) + \alpha\bar{\beta}\log\alpha\bar{\beta}]$$

equals zero. It is easy to note that the function  $f_{\alpha,\beta}(z)$  is a decreasing function of its argument.

We will show two facts:

$$f_{\alpha,\beta}(p(z_L)) \geq 0 \quad (41)$$

$$f_{\alpha,\beta}(p(z_U)) \leq 0, \quad (42)$$

from which we can conclude that  $R_{\alpha,\beta}(z)$  attains its maximum at some  $z \in [z_L, z_U]$ . For the BSC, it needs to be shown that  $f_{\alpha,\alpha}(0.5) \leq 0$  which can be verified easily.

We begin with an explicit calculation of  $f_{\alpha,\beta}(p(z_L))$ :

$$\begin{aligned} f_{\alpha,\beta}(p(z_L)) &\stackrel{(a)}{=} (1 - \alpha\bar{\beta})[H_2(\alpha) - H_2(\beta)] + (\bar{\beta} - \alpha)[2\log(1 - \sqrt{\alpha\bar{\beta}}) - \log(\sqrt{\alpha\bar{\beta}} - \alpha\bar{\beta})(1 + \alpha\bar{\beta}) + \alpha\bar{\beta}\log\alpha\bar{\beta}] \\ &= (1 - \alpha\bar{\beta}) \left[ H_2(\alpha) - H_2(\beta) + (\bar{\beta} - \alpha) \log \left( \frac{1 - \sqrt{\alpha\bar{\beta}}}{\sqrt{\alpha\bar{\beta}}} \right) \right], \end{aligned} \quad (43)$$

where (a) follows from  $p(z_L) = \sqrt{\alpha\bar{\beta}}$ . Since  $1 - \alpha\bar{\beta} \geq 0$ , we need to show that  $\frac{f_{\alpha,\beta}(p(z_L))}{1 - \alpha\bar{\beta}} \geq 0$ .

We now show that the minimal value of (43) is 0. Consider the first derivative, with respect to  $\alpha$ , of  $\frac{f_{\alpha,\beta}(p(z_L))}{1 - \alpha\bar{\beta}}$ :

$$\begin{aligned} \frac{d}{d\alpha} \left[ H_2(\alpha) - H_2(\beta) + (\bar{\beta} - \alpha) \log \left( \frac{1 - \sqrt{\alpha\bar{\beta}}}{\sqrt{\alpha\bar{\beta}}} \right) \right] &= \log \left( \frac{(1 - \alpha)\sqrt{\alpha\bar{\beta}}}{\alpha(1 - \sqrt{\alpha\bar{\beta}})} \right) - \frac{\bar{\beta} - \alpha}{2\alpha(1 - \sqrt{\alpha\bar{\beta}})} \\ &\leq \frac{(1 - \alpha)\sqrt{\alpha\bar{\beta}}}{\alpha(1 - \sqrt{\alpha\bar{\beta}})} - 1 - \frac{\bar{\beta} - \alpha}{2\alpha(1 - \sqrt{\alpha\bar{\beta}})} \\ &= \frac{-(\sqrt{\bar{\beta}} - \sqrt{\alpha})^2}{2\alpha(1 - \sqrt{\alpha\bar{\beta}})} \\ &\leq 0, \end{aligned} \quad (44)$$

where the first inequality follows from  $\log x < x - 1$  for all  $x > 0$  with  $x = \frac{(1 - \alpha)\sqrt{\alpha\bar{\beta}}}{\alpha(1 - \sqrt{\alpha\bar{\beta}})}$ .

Therefore, for each  $\beta$ , the function is non-increasing in  $\alpha$ , so the function can only be decreased if we substitute  $\alpha = \bar{\beta}$ . Since  $f_{\bar{\beta},\beta}(p(z_L)) = 0$ , inequality (41) is proven.

We now use a similar methodology to show (42). The inequality that needs to be shown is

$$\begin{aligned} f_{\alpha,\beta}(p(z_U)) &= (1 - \alpha\bar{\beta})[H_2(\alpha) - H_2(\beta)] + (\bar{\beta} - \alpha)(2\log\sqrt{\alpha\bar{\beta}} + \alpha\bar{\beta}\log\alpha\bar{\beta} - \log(1 - \sqrt{\alpha\bar{\beta}} - \alpha\bar{\beta})(1 + \alpha\bar{\beta})) \\ &\leq 0. \end{aligned} \quad (45)$$

Because it is difficult to prove straightforwardly, we write inequality (45) as a sum of simpler components, i.e.,  $-f_{\alpha,\beta}(p(z_U)) = F_{\alpha,\beta}^1 + F_{\alpha,\beta}^2$ , and we show that  $F_{\alpha,\beta}^1$  and  $F_{\alpha,\beta}^2$  are always non-negative. The functions are:

$$\begin{aligned} F_{\alpha,\beta}^1 &= \alpha\bar{\beta} \left[ (\bar{\beta} - \alpha) \log \left( \frac{1 - \sqrt{\alpha\bar{\beta}} - \alpha\bar{\beta}}{\alpha\bar{\beta}} \right) + H_2(\alpha) - H_2(\beta) \right] \\ F_{\alpha,\beta}^2 &= (\bar{\beta} - \alpha) \log \left( \frac{1 - \sqrt{\alpha\bar{\beta}} - \alpha\bar{\beta}}{\alpha\bar{\beta}} \right) - (H_2(\alpha) - H_2(\beta)) \end{aligned}$$

As before, we take the first derivative of  $F_{\alpha,\beta}^1$ :

$$\begin{aligned}
\frac{d}{d\alpha} \left[ \frac{F_{\alpha,\beta}^1}{\alpha\bar{\beta}} \right] &= (\bar{\beta} - \alpha) \left[ -\frac{1}{\alpha} + \frac{-\bar{\beta} + \frac{\beta}{2\sqrt{\alpha\bar{\beta}}}}{1 - \alpha\bar{\beta} - \sqrt{\alpha\bar{\beta}}} \right] + \log \left( \frac{\bar{\alpha}\bar{\beta}}{1 - \sqrt{\alpha\bar{\beta}} - \alpha\bar{\beta}} \right) \\
&\leq (\bar{\beta} - \alpha) \left[ -\frac{1}{\alpha} + \frac{-\bar{\beta} + \frac{\beta}{2\sqrt{\alpha\bar{\beta}}}}{1 - \alpha\bar{\beta} - \sqrt{\alpha\bar{\beta}}} \right] + \left( \frac{\bar{\alpha}\bar{\beta}}{1 - \sqrt{\alpha\bar{\beta}} - \alpha\bar{\beta}} \right) - 1 \\
&= \frac{(\sqrt{\bar{\alpha}} - \sqrt{\bar{\beta}})\sqrt{\bar{\beta}}}{2\alpha\sqrt{\alpha\bar{\beta}}(1 - \sqrt{\alpha\bar{\beta}} - \alpha\bar{\beta})} [\sqrt{\bar{\alpha}}(\alpha\sqrt{\bar{\beta}} - \bar{\beta}\sqrt{\bar{\alpha}}) + (\alpha\bar{\beta} - \bar{\alpha}\bar{\beta})] \\
&\leq 0,
\end{aligned}$$

where the first inequality follows from  $\log x \leq x - 1$  with  $x = \frac{\bar{\alpha}\bar{\beta}}{1 - \sqrt{\alpha\bar{\beta}} - \alpha\bar{\beta}}$ . The last inequality follows from  $\alpha \leq \bar{\beta}$ , which implies, in turn,  $\alpha\sqrt{\bar{\beta}} - \bar{\beta}\sqrt{\bar{\alpha}} \leq 0$  and  $\alpha\bar{\beta} - \bar{\alpha}\bar{\beta} \leq 0$ . We thus conclude that  $F_{\alpha,\beta}^1$  is non-increasing in  $\alpha$ , and therefore, if we take  $\alpha$  to be  $1 - \beta$ , we get its minimal value. Note that  $F_{\bar{\beta},\beta}^1 = 0$ , so we have  $F_{\alpha,\beta}^1 \geq 0$ .

Now we take the derivative of  $F_{\alpha,\beta}^2$  with respect to  $\beta$ :

$$\begin{aligned}
\frac{d}{d\beta} F_{\alpha,\beta}^2 &= \frac{(\beta - \bar{\alpha})\sqrt{\bar{\alpha}\bar{\beta}}(-\beta + 2\sqrt{\beta\bar{\alpha}})}{2\beta^2(1 - \alpha\bar{\beta} - \sqrt{\alpha\bar{\beta}})} + \log \left( \frac{\bar{\alpha}\bar{\beta}}{1 - \alpha\bar{\beta} - \sqrt{\alpha\bar{\beta}}} \right) \\
&\leq \frac{(\beta - \bar{\alpha})\sqrt{\bar{\alpha}}(-\sqrt{\bar{\beta}} + 2\sqrt{\bar{\alpha}})}{2\beta(1 - \alpha\bar{\beta} - \sqrt{\beta\bar{\alpha}})} + \left( \frac{\bar{\alpha}\bar{\beta}}{1 - \alpha\bar{\beta} - \sqrt{\alpha\bar{\beta}}} \right) - 1 \\
&= \frac{(\sqrt{\bar{\beta}} - \sqrt{\bar{\alpha}})}{2\beta(1 - \alpha\bar{\beta} - \sqrt{\alpha\bar{\beta}})} (\bar{\alpha}\sqrt{\bar{\beta}} + 2\beta\sqrt{\bar{\beta}} + \sqrt{\bar{\alpha}}(2\bar{\alpha} - \beta)) \\
&\leq 0.
\end{aligned}$$

The last inequality follows from  $\sqrt{\bar{\beta}} - \sqrt{\bar{\alpha}} \leq 0$ . Repeating the same steps as was done for  $F_{\alpha,\beta}^1$ , we find that  $F_{\alpha,\beta}^2 \geq 0$ , which, in turn, gives that  $-f_{\alpha,\beta}(p(z_U)) \geq 0$  as required.  $\blacksquare$

## APPENDIX B PROOF OF THEOREM 3

Throughout this section, we use  $x = \alpha\bar{\alpha}$ , and  $x', x''$  to stand for the first and second derivatives of  $x$ , respectively. Recall that  $p_\alpha$  in Corollary 1 is the solution for  $(\alpha\bar{\alpha}) \log(\alpha\bar{\alpha}) + 2 \log(1 - p) = (1 + \alpha\bar{\alpha}) \log(p - \alpha\bar{\alpha})$ , and let  $p'_\alpha$  denote its first derivative. The next lemma concerns  $p'_\alpha$  and is the foundation for the proof of Theorem 3.

**Lemma 6.** *The first derivative of  $p_\alpha$  is:*

$$\begin{aligned}
p'_\alpha &= (1 - 2\alpha) \frac{(1 - p_\alpha)(p_\alpha - \alpha\bar{\alpha})}{(\alpha\bar{\alpha} - 1)(1 + p_\alpha)} \left[ \log \left( \frac{p_\alpha - \alpha\bar{\alpha}}{\bar{\alpha}} \right) - \log \alpha \right] + (1 - 2\alpha) \frac{1 - p_\alpha}{1 - \alpha\bar{\alpha}} \\
&\triangleq K_2(\alpha) - K_1(\alpha) \log \alpha,
\end{aligned}$$

with the defined functions:

$$\begin{aligned}
K_1(\alpha) &\triangleq (1 - 2\alpha) \frac{(1 - p_\alpha)(p_\alpha - \alpha\bar{\alpha})}{(\alpha\bar{\alpha} - 1)(1 + p_\alpha)} \\
K_2(\alpha) &\triangleq K_1(\alpha) \log \left( \frac{p_\alpha - \alpha\bar{\alpha}}{\bar{\alpha}} \right) + (1 - 2\alpha) \frac{1 - p_\alpha}{1 - \alpha\bar{\alpha}}.
\end{aligned}$$

Note that  $p_0 = 2 - \lambda$ , so  $K_1(\alpha)$  and  $K_2(\alpha)$  are defined at  $\alpha = 0$ :

$$K_1(0) = -\frac{p_0(1-p_0)}{1+p_0}$$

$$K_2(0) = K_1(0) \log p_0 + 1 - p_0.$$

*Proof of Lemma 6:* We calculate the first derivative for each side of  $2 \log(1 - p_\alpha) = (1 + \alpha \bar{\alpha}) \log(p_\alpha - \alpha \bar{\alpha}) - (\alpha \bar{\alpha}) \log(\alpha \bar{\alpha})$  so we have:

$$\frac{-2}{1-p_\alpha} p'_\alpha = x' \left[ \log \left( \frac{p_\alpha - x}{x} \right) - \frac{1+p_\alpha}{p_\alpha - x} \right] + \frac{1+x}{p_\alpha - x} p'_\alpha. \quad (46)$$

Arranging both sides of (46) gives the desired equation:

$$p'_\alpha = (1-2\alpha) \frac{(1-p_\alpha)(p_\alpha - \alpha \bar{\alpha})}{(\alpha \bar{\alpha} - 1)(1+p_\alpha)} \log \left( \frac{p_\alpha - \alpha \bar{\alpha}}{\alpha \bar{\alpha}} \right) + (1-2\alpha) \frac{1-p_\alpha}{1-\alpha \bar{\alpha}}.$$

■

The next lemma is technical and is made to shorten the proof of Theorem 3:

**Lemma 7.** Define  $K_3(\alpha) = \frac{x'}{1+p_\alpha}$ , then it can be expressed as

$$K_3(\alpha) = \frac{1}{1+p_0} + N\alpha \log \alpha + o(\alpha \log \alpha),$$

where  $N$  is a constant.

The proof of Lemma 7 appears in Appendix B-A. We are now ready to prove the main result of this section.

*Proof of Theorem 3:* Consider the next chain of equalities:

$$\begin{aligned} & C^{\text{BSC}}(\alpha) + H_2(\alpha) + K_3(\alpha) \alpha \log \alpha \\ & \stackrel{(a)}{=} \log(1 - p_\alpha) - \log(p_\alpha - x) + K_3(\alpha) \alpha \log \alpha \\ & \stackrel{(b)}{=} \log \left( \frac{1-p_0}{p_0} \right) + \left[ \frac{-p'_\alpha}{1-p_\alpha} - \frac{p'_\alpha - x'}{p_\alpha - x} + K'_3(\alpha) \alpha \log \alpha + K_3(\alpha) [1 + \log \alpha] \right]_{\alpha=0} \alpha + o(\alpha) \\ & \stackrel{(c)}{=} \log \left( \frac{1-p_0}{p_0} \right) + \left[ p'_\alpha \frac{x-1}{(1-p_\alpha)(p_\alpha - x)} + \frac{x'}{p_\alpha - x} + K_3(\alpha) [1 + \log \alpha] \right]_{\alpha=0} \alpha + o(\alpha) \\ & \stackrel{(d)}{=} \log \left( \frac{1-p_0}{p_0} \right) + \left[ [K_2(\alpha) - K_1(\alpha) \log \alpha] \frac{x-1}{(1-p_\alpha)(p_\alpha - x)} + \frac{x'}{p_\alpha - x} + K_3(\alpha) [1 + \log \alpha] \right]_{\alpha=0} \alpha + o(\alpha) \\ & \stackrel{(e)}{=} \log \left( \frac{1-p_0}{p_0} \right) + M\alpha + \left[ K_1(\alpha) \log \alpha \frac{1-x}{(1-p_\alpha)(p_\alpha - x)} + K_3(\alpha) \log \alpha \right]_{\alpha=0} \alpha + o(\alpha) \\ & = \log \left( \frac{1-p_0}{p_0} \right) + M\alpha + \left[ \frac{-x'}{1+p_\alpha} \log \alpha + K_3(\alpha) \log \alpha \right]_{\alpha=0} \alpha + o(\alpha) \\ & = \log \left( \frac{1-p_0}{p_0} \right) + M\alpha + o(\alpha) \end{aligned} \quad (47)$$

where:

- (a) follows from Corollary 1;
- (b) follows from the Taylor series approximation  $f(\alpha) = f(0) + f'(0)\alpha + O(\alpha^2)$ ;
- (c) follows from Lemma 7, specifically,  $\lim_{\alpha \rightarrow 0} K'_3(\alpha) \alpha \log \alpha = 0$ ;

(d) follows from Lemma 6, specifically,  $p'_\alpha = K_2(\alpha) - K_1(\alpha) \log \alpha$ ;

(e) follows from the notation  $M \triangleq K_2(0) \frac{-1}{(1-p_0)(p_0)} + \frac{1}{p_0} + K_3(0)$ .

Thus, we have from (47) that  $C^{\text{BSC}}(\alpha) + H_2(\alpha) + K_3(\alpha)\alpha \log \alpha = \log\left(\frac{1-p_0}{p_0}\right) + M\alpha + o(\alpha)$ .

The derivation is completed with the following equalities:

$$\begin{aligned} C^{\text{BSC}}(\alpha) &= \log\left(\frac{1-p_0}{p_0}\right) - K_3(\alpha)\alpha \log \alpha - H_2(\alpha) + M\alpha + o(\alpha) \\ &\stackrel{(a)}{=} \log \lambda - [K_3(0) + N\alpha \log \alpha + o(\alpha \log \alpha)]\alpha \log \alpha - H_2(\alpha) + M\alpha + o(\alpha) \\ &\stackrel{(b)}{=} \log \lambda + \frac{2-\lambda}{3-\lambda}\alpha \log \alpha + \left(\frac{\log(2-\lambda) - (2-\lambda)}{3-\lambda}\right)\alpha + O(\alpha^2 \log^2 \alpha) \end{aligned}$$

where:

(a) follows from  $p_0 = 2 - \lambda$  and Lemma 7;

(b) follows from  $H_2(\alpha) = \alpha - \alpha \log \alpha + o(\alpha)$  and arranging the equation. ■

#### A. Proof of Lemma 7

By a Taylor series approximation, we have

$$\begin{aligned} &\frac{x'}{1+p_\alpha} - \frac{x'K_1(\alpha)}{(1+p_\alpha)^2}\alpha \log \alpha \\ &= \frac{1}{1+p_0} + \left[ \frac{x''}{1+p_\alpha} - p'_\alpha \frac{x'}{(1+p_\alpha)^2} - \left( \frac{x'K_1(\alpha)}{(1+p_\alpha)^2} \right)' \alpha \log \alpha - \frac{x'K_1(\alpha)}{(1+p_\alpha)^2}(1 + \log \alpha) \right]_{\alpha=0} \alpha + o(\alpha) \\ &\stackrel{(a)}{=} \frac{1}{1+p_0} + C\alpha + \left[ -p'_\alpha \frac{x'}{(1+p_\alpha)^2} - \frac{x'K_1(\alpha)}{(1+p_\alpha)^2} \log \alpha \right]_{\alpha=0} \alpha + o(\alpha) \\ &\stackrel{(b)}{=} \frac{1}{1+p_0} + C\alpha + \left[ K_2(\alpha) \frac{-x'}{(1+p_\alpha)^2} \right]_{\alpha=0} \alpha + o(\alpha) \\ &\stackrel{(c)}{=} \frac{1}{1+p_0} + \tilde{C}\alpha + o(\alpha) \end{aligned}$$

where (a) follows from the fact that  $\lim_{\alpha \rightarrow 0} \left( \frac{x'K_1(\alpha)}{(1+p_\alpha)^2} \right)' \alpha \log \alpha = 0$  and the notation  $C = \frac{-2}{1+p_0} - \frac{K_1(0)}{(1+p_0)^2}$ , (b) follows from  $p'_\alpha = K_2(\alpha) - K_1(\alpha)\alpha \log \alpha$ , and finally, (c) follows from the notation  $\tilde{C} = C - \frac{K_2(0)}{(1+p_0)^2}$ .

So, we have that

$$\frac{x'}{1+p_\alpha} = \frac{1}{1+p_0} + \tilde{C}\alpha + o(\alpha) + \frac{x'K_1(\alpha)}{(1+p_\alpha)^2}\alpha \log \alpha.$$

Applying the Taylor series approximation once again on  $\frac{x'K_1(\alpha)}{(1+p_\alpha)^2}$  gives that:

$$\frac{x'K_1(\alpha)}{(1+p_\alpha)^2} = \frac{K_1(0)}{(1+p_0)^2} + h(\alpha),$$

where  $h(\alpha)$  is some function such that  $\lim_{\alpha \rightarrow 0} h(\alpha) = 0$ .

TABLE II  
THE FUNCTIONS  $\text{ARG1}(z)$  AND  $\text{ARG2}(z)$

|     | domain       | $\tilde{h}(\text{arg1}(z))$          | $\tilde{h}(\text{arg2}(z))$          |
|-----|--------------|--------------------------------------|--------------------------------------|
| I   | $[0, z_1]$   | $\tilde{\rho}_{\alpha,\beta}$        | $\tilde{\rho}_{\alpha,\beta}$        |
| II  | $[z_1, z_2]$ | $\tilde{\rho}_{\alpha,\beta}$        | $h_2^{\alpha,\beta}(\text{arg2}(z))$ |
| III | $[z_2, z_3]$ | $\tilde{\rho}_{\alpha,\beta}$        | $h_1^{\alpha,\beta}(\text{arg2}(z))$ |
| IV  | $[z_3, z_4]$ | $h_2^{\alpha,\beta}(\text{arg1}(z))$ | $h_1^{\alpha,\beta}(\text{arg2}(z))$ |
| V   | $[z_4, 1]$   | $h_1^{\alpha,\beta}(\text{arg1}(z))$ | $h_1^{\alpha,\beta}(\text{arg2}(z))$ |

Combining the last two derivations, we have the required equality, i.e.,

$$\begin{aligned} \frac{x'}{1+p_\alpha} &= \frac{1}{1+p_0} + \tilde{C}\alpha + o(\alpha) + \left[ \frac{K_1(0)}{(1+p_0)^2} + h(\alpha) \right] \alpha \log \alpha \\ &= \frac{1}{1+p_0} + N\alpha \log \alpha + o(\alpha \log \alpha), \end{aligned}$$

where  $N = \frac{K_1(0)}{(1+p_0)^2}$ . ■

## APPENDIX C

### PROOF OF THEOREM 10

The following lemma is technical and is useful for understanding the structure of  $\tilde{h}_{\alpha,\beta}(z)$ .

**Lemma 8.** For all  $[\alpha, \beta] \in [0, 1] \times [0, 1]$  s.t.  $\alpha + \beta \leq 1$ ,

- 1) The function  $\tilde{h}_{\alpha,\beta}(z)$  is continuous on  $[0, 1]$ .
- 2) The function  $\tilde{h}_{\alpha,\beta}(z)$  is concave on  $[0, 1]$ .
- 3) The only maximum of  $h_2^{\alpha,\beta}(z)$  is attained at  $z = z_2^{\alpha,\beta}$ , and its value is  $\tilde{\rho}_{\alpha,\beta}$ .
- 4) The first derivative of  $h_1^{\alpha,\beta}(z)$  is non-negative for  $z \in [0, z_1^{\alpha,\beta}]$ .

The proof of Lemma 8 appears in Appendix C-A.

*Proof of Theorem 10:* The function  $\tilde{h}_{\alpha,\beta}(z)$  is defined as a concatenation of  $h_1^{\alpha,\beta}(z)$ ,  $h_2^{\alpha,\beta}(z)$ , and  $\tilde{\rho}_{\alpha,\beta}$ ; to simplify the calculation of  $(T\tilde{h}_{\alpha,\beta})(z)$ , the unit interval is partitioned into non-intersecting sub-intervals, where each sub-interval uniquely determines the function  $\tilde{h}_{\alpha,\beta}(\text{argi}(z))$  to be  $h_1^{\alpha,\beta}(z)$ ,  $h_2^{\alpha,\beta}(z)$  or  $\tilde{\rho}_{\alpha,\beta}$ , for  $i = 1, 2$ . Since there are two concatenation points,  $z_1^{\alpha,\beta}$  and  $z_2^{\alpha,\beta}$ , the unit interval is partitioned at the set of points that satisfy,

$$\begin{aligned} \text{arg1}_{\alpha,\beta}(z) &= z_i^{\alpha,\beta} \\ \text{arg2}_{\alpha,\beta}(z) &= z_i^{\alpha,\beta}, \end{aligned} \tag{48}$$

for  $i = 1, 2$ .

Calculation of the points in (48) reveals that the unit interval should be partitioned at  $z_1^{\alpha,\beta}$ ,  $z_2^{\alpha,\beta}$ ,  $z_3^{\alpha,\beta}$ ,  $z_4^{\alpha,\beta}$  from (15). Fig. 7 illustrates the argument functions and the partitions when  $\alpha = \beta = 0.25$ . As can be seen from Fig. 7,

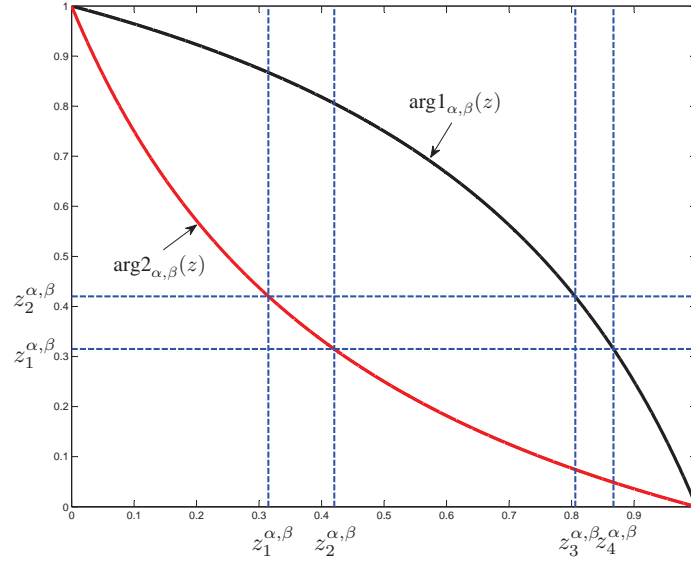


Fig. 7. Illustration of the argument functions as a function of  $z$ , for  $\alpha = \beta = 0.25$ .

five segments need to be considered when calculating  $(T\tilde{h}_{\alpha,\beta})(z)$ . The relevant segments are summarized in Table II together with  $\tilde{h}_{\alpha,\beta}(\text{argi}(z))$  for  $i = 1, 2$  for each sub-interval.

Now, the operator  $T\tilde{h}_{\alpha}(z)$  can be calculated, such that in each calculation, we restrict actions to one sub-interval from Table II. For the interval I, i.e.,  $z \in [0, z_1^{\alpha,\beta})$ ,

$$\begin{aligned}
 & (T\tilde{h}_{\alpha,\beta})(z) \\
 &= \sup_{0 \leq \delta \leq z} H_2(p(\delta)) - (1 - \delta)H_2(\alpha) - \delta H_2(\beta) + (1 - p(\delta))h_{\alpha,\beta}(\text{arg1}(\delta)) + p(\delta)h_{\alpha,\beta}(\text{arg2}(\delta)) \\
 &\stackrel{(a)}{=} \sup_{0 \leq \delta \leq z} H_2(p(\delta)) - (1 - \delta)H_2(\alpha) - \delta H_2(\beta) + (1 - p(\delta))\tilde{\rho}_{\alpha,\beta} + p(\delta)\tilde{\rho}_{\alpha,\beta} \\
 &\stackrel{(b)}{=} \sup_{0 \leq \delta \leq z} h_1(\delta) + \tilde{\rho}_{\alpha,\beta} \\
 &\stackrel{(c)}{=} h_1(z) + \tilde{\rho}_{\alpha,\beta}
 \end{aligned} \tag{49}$$

where (a) follows from the restriction of  $z \in [0, z_1]$  and substituting the functions from Table II, (b) follows from the definition of  $h_1(\delta)$  in (39) and (c) follows from Item 4) of Lemma 8, specifically,  $h_1^{\alpha,\beta}(z)$  is non-decreasing on  $[0, z_1^{\alpha,\beta}]$ . Note that the maximizer is  $\delta(z) = z$ .

The operator with actions restricted to interval II, i.e.,  $\delta \in [z_1^{\alpha,\beta}, z]$  for  $z \in [z_1^{\alpha,\beta}, z_2^{\alpha,\beta}]$  is:

$$\begin{aligned}
 & \sup_{z_1 \leq \delta \leq z} H_2(p(\delta)) - (1 - \delta)H_2(\alpha) - \delta H_2(\beta) + (1 - p(\delta))\tilde{h}_{\alpha,\beta}(\text{arg1}(\delta)) + p(\delta)\tilde{h}_{\alpha,\beta}(\text{arg2}(\delta)) \\
 &\stackrel{(a)}{=} \sup_{z_1 \leq \delta \leq z} X(\delta) + p(\delta)\tilde{\rho}_{\alpha,\beta} + (1 - p(\delta))\tilde{\rho}_{\alpha,\beta} + \left[ \frac{p(\delta)X(\text{arg2}(\delta)) + \alpha\tilde{\rho}_{\alpha,\beta}X(\delta)}{1 - \alpha\tilde{\rho}_{\alpha,\beta}} \right]
 \end{aligned}$$

$$\begin{aligned}
&\stackrel{(b)}{=} \sup_{z_1 \leq \delta \leq z} h_2(\delta) + \tilde{\rho}_{\alpha,\beta} \\
&\stackrel{(c)}{=} h_2(z) + \tilde{\rho}_{\alpha,\beta},
\end{aligned} \tag{50}$$

where (a) follows from the definition of  $X(\delta)$  in (39) and Table II, (b) follows the expression for  $h_2(\delta)$  in (39) and (c) follows from Item 3) in Lemma 8, where it was shown that  $h_2(z)$  is increasing on  $[0, z_2^{\alpha,\beta}]$ .

To conclude the calculation of  $(T\tilde{h}_{\alpha,\beta})(z)$  for  $z \in [z_1^{\alpha,\beta}, z_2^{\alpha,\beta}]$ , consider

$$\begin{aligned}
(T\tilde{h}_{\alpha,\beta})(z) &\stackrel{(a)}{=} \max\left(\sup_{z \in [0, z_1]} h_1(z) + \tilde{\rho}_{\alpha,\beta}, \sup_{z \in [z_1, z]} h_2(z) + \tilde{\rho}_{\alpha,\beta}\right) \\
&\stackrel{(b)}{=} \max(h_1(z_1), h_2(z)) + \tilde{\rho}_{\alpha,\beta} \\
&\stackrel{(c)}{=} h_2(z) + \tilde{\rho}_{\alpha,\beta},
\end{aligned} \tag{51}$$

where (a) follows from (49) and (50), and both (b) and (c) follow from Items 3) and 4) in Lemma 8. Note also here that the maximizer of  $(T\tilde{h}_{\alpha,\beta})(z)$  for  $z$  on sub-interval II is  $\delta(z) = z$ .

For actions that are restricted to interval III, i.e.,  $\delta \in [z_2^{\alpha,\beta}, z]$  with  $z \in [z_2^{\alpha,\beta}, z_3^{\alpha,\beta}]$ , consider

$$\begin{aligned}
&\sup_{z_2 \leq \delta \leq z} H_2(p(\delta)) - (1 - \delta)H_2(\alpha) - \delta H_2(\beta) + (1 - p(\delta))\tilde{h}_{\alpha,\beta}(\arg 1(\delta)) + p(\delta)\tilde{h}_{\alpha,\beta}(\arg 2(\delta)) \\
&\stackrel{(a)}{=} \sup_{z_2 \leq \delta \leq z} X(\delta) + \tilde{\rho}_{\alpha,\beta} + p(\delta) \left[ X(\arg 2_{\alpha,\beta}(\delta)) + \left( \frac{\alpha\bar{\beta}}{p(\delta)} \right) \tilde{\rho}_{\alpha,\beta} \right] \\
&\stackrel{(b)}{=} \tilde{\rho}_{\alpha,\beta} + \tilde{\rho}_{\alpha,\beta},
\end{aligned} \tag{52}$$

where (a) follows from the definition of  $X(\delta)$  in (39) and Table II and (b) follows from Item 3) in Lemma 8, specifically,  $h_2(z)$  achieves its maximum value at  $z = z_2$ . Note from (51) and (52) that the operator on III satisfies  $(T\tilde{h}_{\alpha,\beta})(z) = 2\tilde{\rho}_{\alpha,\beta}$  and that the maximizer is  $\delta(z) = z_2$ .

For the action restricted on interval IV, i.e.,  $\delta \in [z_3, z]$  with  $z \in [z_3, z_4]$ , consider

$$\begin{aligned}
&\sup_{z_3 \leq \delta \leq z} H_2(p(\delta)) - (1 - \delta)H_2(\alpha) - \delta H_2(\beta) + (1 - p(\delta))\tilde{h}_{\alpha,\beta}(\arg 1(\delta)) + p(\delta)\tilde{h}_{\alpha,\beta}(\arg 2(\delta)) \\
&\stackrel{(a)}{=} \sup_{z_3 \leq \delta \leq z} X(\delta) + p(\delta)\tilde{\rho}_{\alpha,\beta} + (1 - p(\delta))h_2(\arg 1_{\alpha,\beta}(\delta)) + p(\delta) \left[ X(\arg 2(\delta)) + \frac{\alpha\bar{\beta}}{p(\delta)}\tilde{\rho}_{\alpha,\beta} \right] \\
&\stackrel{(b)}{\leq} \tilde{\rho}_{\alpha,\beta} + \tilde{\rho}_{\alpha,\beta},
\end{aligned} \tag{53}$$

where (a) follows from the definition of  $X(\delta)$  in (39) and Table II and (b) follows from  $h_2(z) \leq \tilde{\rho}_{\alpha,\beta}$  shown in Item 3), Lemma 8.

The calculation of the last interval,  $[z_4, 1]$ , is omitted here, but it follows the same repeated arguments, so we have  $(T\tilde{h}_{\alpha,\beta})(z) \leq 2\tilde{\rho}_{\alpha,\beta}$ . Now, Item 3) in Lemma 8 together with (53) gives us that  $(T\tilde{h}_{\alpha,\beta})(z) = 2\tilde{\rho}_{\alpha,\beta}$  also for  $z \in [z_2, z_4]$ . To conclude, we have shown that  $(T\tilde{h}_{\alpha,\beta})(z) = \tilde{h}_{\alpha,\beta}(z) + \tilde{\rho}_{\alpha,\beta}$ .

#### A. Proof of Lemma 8

Throughout this section, we use  $z_i$  as shorthand for  $z_i^{\alpha,\beta}$  and  $p^{\text{opt}}$  stands for  $p(z_2^{\alpha,\beta})$ .



**Continuity:** Each of the functions defining  $\tilde{h}_{\alpha,\beta}(z)$  is continuous, and therefore, one should verify that the concatenation points satisfy

$$\begin{aligned} h_1^{\alpha,\beta}(z_1) &= h_2^{\alpha,\beta}(z_1) \\ h_2^{\alpha,\beta}(z_2) &= \tilde{\rho}_{\alpha,\beta}. \end{aligned} \quad (54)$$

The second equality in (54) is verified as follows:

$$\begin{aligned} &(1 - \alpha\bar{\beta})h_2^{\alpha,\beta}(z_2) \\ &= X(z_2) + p^{\text{opt}}X(\arg_2(z_2)) \\ &= H_2(p^{\text{opt}}) + p^{\text{opt}}H_2\left(\frac{\alpha\bar{\beta}}{p^{\text{opt}}}\right) - (\bar{z}_2 + \bar{\beta}z_2)H_2(\alpha) - (z_2 + \alpha\bar{z}_2)H_2(\beta) - (p^{\text{opt}} + \alpha\bar{\beta})\tilde{\rho}_{\alpha,\beta} \\ &= (1 - \alpha\bar{\beta})\tilde{\rho}_{\alpha,\beta}, \end{aligned}$$

and since  $(1 - \alpha\bar{\beta}) \neq 0$ , it follows that  $h_2^{\alpha,\beta}(z_2) = \tilde{\rho}_{\alpha,\beta}$ . This derivation also gives us that

$$\begin{aligned} \tilde{\rho}_{\alpha,\beta} &= h_2^{\alpha,\beta}(z_2) \\ &\stackrel{(a)}{=} \frac{X(z_2) + p^{\text{opt}}X(z_1)}{1 - \alpha\bar{\beta}}, \end{aligned} \quad (55)$$

where (a) follows from the fact that  $z_1 = \arg_2(z_2)$ .

The value of  $h_2^{\alpha,\beta}(z_1)$  is

$$\begin{aligned} h_2^{\alpha,\beta}(z_1) &= \frac{X(z_1) + \frac{\alpha\bar{\beta}}{p^{\text{opt}}}X(z_2)}{1 - \alpha\bar{\beta}} \\ &\stackrel{(a)}{=} \frac{1}{p^{\text{opt}}}[\tilde{\rho}_{\alpha,\beta} - X(z_2)] \\ &= H_2\left(\frac{\alpha\bar{\beta}}{p^{\text{opt}}}\right) - \frac{\bar{\beta}z_2}{p^{\text{opt}}}H_2(\alpha) - \frac{\alpha\bar{z}_2}{p^{\text{opt}}}H_2(\beta) \\ &= H_2\left(\frac{\alpha\bar{\beta}}{p^{\text{opt}}}\right) - \bar{z}_1H_2(\alpha) - z_1H_2(\beta) \end{aligned} \quad (56)$$

where (a) follows from (55).

From (39), we have that

$$h_1^{\alpha,\beta}(z_1) = H_2\left(\frac{\alpha\bar{\beta}}{p^{\text{opt}}}\right) - \bar{z}_1H_2(\alpha) - z_1H_2(\beta), \quad (57)$$

which together with (56) concludes the continuity of  $\tilde{h}_{\alpha,\beta}(z)$  at  $z = z_1$ .

**Concavity:** First, we show that each element in  $\tilde{h}_{\alpha,\beta}(z)$  is concave and then we argue that the concatenation of these functions is also concave. The function  $h_1^{\alpha,\beta}(z)$  is concave since it is a composition of the binary entropy function, which is concave, with an affine function. The function  $h_2^{\alpha,\beta}(z)$  can be written explicitly from (39), and then all of its elements are linear except for the entropy function which is concave and the expression  $p(z)H_2\left(\frac{\alpha\bar{z}}{p(z)}\right)$ . The latter expression is also concave since it is known that the perspective of the concave function  $H_2(z)$ , that is,  $tf\left(\frac{x}{t}\right)$  for  $t > 0$  is also concave. Therefore, each element comprising  $\tilde{h}_{\alpha,\beta}(z)$  is concave.

It was shown in [13, Lemma 5] that a continuous concatenation of concave functions is concave if the one-sided derivatives at the concatenation points are equal. Therefore,  $\tilde{h}_{\alpha,\beta}(z)$  is concave if the following conditions are satisfied:

$$h'_1(z_1) = h'_2(z_1) \quad (58)$$

$$h'_2(z_2) = 0. \quad (59)$$

An auxiliary relation is derived by using the derivative of  $R_{\alpha,\beta}(z)$

$$\begin{aligned} \frac{d}{dz} R_{\alpha,\beta}(z) &= \frac{(p'H'_2(p) + [pH_2\left(\frac{\alpha\bar{\beta}}{p}\right)]' + \beta H_2(\alpha) - \bar{\alpha} H_2(\beta))(1+p) - p'(1+p)R_{\alpha,\beta}(z)}{(1+p)^2} \\ &= \frac{p'H'_2(p) + [pH_2\left(\frac{\alpha\bar{\beta}}{p}\right)]' + \beta H_2(\alpha) - \bar{\alpha} H_2(\beta) - p'R_{\alpha,\beta}(z)}{1+p}, \end{aligned} \quad (60)$$

where  $p'$  is first derivative of  $p(z)$ . Since  $z_2^{\alpha,\beta}$  is the maximum of  $R_{\alpha,\beta}(z)$ , the numerator of (60) is equal to zero at this point (one can verify that  $R_{\alpha,\beta}(z) = 0$  when  $z = 0$  or  $z = 1$ ), and one can obtain the relation

$$p'H'_2(p^{\text{opt}}) + \left[pH_2\left(\frac{\alpha\bar{\beta}}{p}\right)\right]'\bigg|_{p=p^{\text{opt}}} = -\beta H_2(\alpha) + \bar{\alpha} H_2(\beta) + p'\tilde{\rho}_{\alpha,\beta} \quad (61)$$

The following calculations are also necessary:

$$\begin{aligned} X'(z) &= p'H'_2(p) + H_2(\alpha) - H_2(\beta) - p'\tilde{\rho}_{\alpha,\beta} \\ X(\arg 2(z)) &= H_2\left(\frac{\alpha\bar{\beta}}{p}\right) - \overline{\arg 2(z)}H_2(\alpha) - \arg 2(z)H_2(\beta) - \frac{\alpha\bar{\beta}}{p}\tilde{\rho}_{\alpha,\beta} \\ X'(\arg 2(z)) &= p'H'_2\left(\frac{\alpha\bar{\beta}}{p}\right) + H_2(\alpha) - H_2(\beta) - p'\tilde{\rho}_{\alpha,\beta} \end{aligned}$$

where derivatives are taken with respect to  $z$ .

The first derivative of  $h_2(z)$  is:

$$\begin{aligned} &\frac{d}{dz}((1 - \alpha\bar{\beta})h_2^{\alpha,\beta}(z)) \\ &= X'(z) + p'X(\arg 2(z)) + p\arg 2'(z)X'(\arg 2(z)) \\ &= p'H'_2(p) + p'H_2\left(\frac{\alpha\bar{\beta}}{p}\right) - \frac{\alpha\bar{\beta}}{p}p'H'_2\left(\frac{\alpha\bar{\beta}}{p}\right) + H_2(\alpha) - H_2(\beta) - p'\tilde{\rho}_{\alpha,\beta} \\ &\quad + p'\left[-\overline{\arg 2(z)}H_2(\alpha) - \arg 2(z)H_2(\beta)\right] - \frac{\alpha\bar{\beta}}{p}[H_2(\alpha) - H_2(\beta)]. \end{aligned} \quad (62)$$

Substituting  $z = z_2$  into (62) and using (61) we obtain the desired equality

$$(1 - \alpha\bar{\beta})\frac{d}{dz}h_2^{\alpha,\beta}(z)\bigg|_{z=z_2} = 0.$$

For the other condition, (59), one can show that  $p(z_1^{\alpha,\beta}) = \frac{\alpha\bar{\beta}}{p(z_2)}$ , which results in

$$(1 - \alpha\bar{\beta})\frac{d}{dz}h_2^{\alpha,\beta}(z)\bigg|_{z=z_1} = (1 - \alpha\bar{\beta})[p'H'_2\left(\frac{\alpha\bar{\beta}}{p^{\text{opt}}}\right) + H_2(\alpha) - H_2(\beta)]$$

The derivative of  $h_1^{\alpha,\beta}(z)$  at  $z = z_1$  is:

$$\frac{d}{dz}h_1^{\alpha,\beta}(z_1) = p'H_2'\left(\frac{\alpha\bar{\beta}}{p^{\text{opt}}}\right) + H_2(\alpha) - H_2(\beta),$$

and this concludes the concavity of  $\tilde{h}_{\alpha,\beta}(z)$ .

The last two items in Lemma 8 follow from the concavity of  $\tilde{h}_{\alpha,\beta}(z)$  and the fact that  $z_1 \leq z_2$ : since the maximum is at  $z_2$ , then the derivative of  $h_2^{\alpha,\beta}(z)$  at  $z_1$  is positive and equals the derivative of  $h_1^{\alpha,\beta}(z)$  at  $z_1$ . ■

## REFERENCES

- [1] O. Sabag, H. H. Permuter, and N. Kashyap, "The feedback capacity of the BIBO channel with a no-consecutive-ones input constraint," in *Int. Conf. on Signal Processing and Communications (SPCOM)*, June 2016.
- [2] M. Horstein, "Sequential transmission using noiseless feedback," *IEEE Trans. Inf. Theory*, vol. 9, no. 3, pp. 136–143, Jul. 1963.
- [3] O. Shayevitz and M. Feder, "Optimal feedback communication via posterior matching," *IEEE Trans. Inf. Theory*, vol. 57, no. 3, pp. 1186–1222, Mar. 2011.
- [4] P. Vontobel, A. Kavcic, D. Arnold, and H.-A. Loeliger, "A generalization of the Blahut-Arimoto algorithm to finite-state channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 5, pp. 1887–1918, May 2008.
- [5] G. Han and B. Marcus, "Asymptotics of entropy rate in special families of hidden Markov chains," *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1287–1295, Mar. 2010.
- [6] E. Zehavi and J. Wolf, "On runlength codes," *IEEE Trans. Inf. Theory*, vol. 34, no. 1, pp. 45–54, Jan. 1988.
- [7] G. Han and B. Marcus, "Concavity of the mutual information rate for input-restricted memoryless channels at high SNR," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1534–1548, Mar. 2012.
- [8] Y. Li and G. Han, "Input-constrained erasure channels: Mutual information and capacity," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, June 2014, pp. 3072–3076.
- [9] S. Yang, A. Kavčić, and S. Tatikonda, "Feedback capacity of finite-state machine channels," *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 799–810, Mar. 2005.
- [10] S. C. Tatikonda, "Control under communication constraints," Ph.D. dissertation, Massachusetts Institute of Technology, Cambridge, MA, 2000.
- [11] S. Tatikonda and S. Mitter, "The capacity of channels with feedback," *IEEE Trans. Inf. Theory*, vol. 55, no. 1, pp. 323–349, Jan. 2009.
- [12] H. H. Permuter, P. Cuff, B. V. Roy, and T. Weissman, "Capacity of the trapdoor channel with feedback," *IEEE Trans. Inf. Theory*, vol. 54, no. 7, pp. 3150–3165, Jul. 2009.
- [13] O. Elishco and H. Permuter, "Capacity and coding for the Ising channel with feedback," *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5138–5149, Sep. 2014.
- [14] O. Sabag, H. Permuter, and N. Kashyap, "The feedback capacity of the binary erasure channel with a no-consecutive-ones input constraint," *IEEE Trans. Inf. Theory*, vol. 62, no. 1, pp. 8–22, Jan 2016.
- [15] J. Wu and A. Anastopoulos, "On the capacity of the general trapdoor channel with feedback," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2016, pp. 2256–2260.
- [16] A. Sharov and R. M. Roth, "On the capacity of generalized ising channels," *IEEE Trans. on Inf. Theory*, vol. PP, no. 99, pp. 1–1, Dec. 2016.
- [17] J. Chen and T. Berger, "The capacity of finite-state Markov channels with feedback," *IEEE Trans. Inf. Theory*, vol. 51, pp. 780–789, 2005.
- [18] C. Shannon, "The zero error capacity of a noisy channel," *IEEE Trans. Inf. Theory*, vol. 2, no. 3, pp. 8–19, Sep. 1956.
- [19] G. Han and B. Marcus, "Asymptotics of input-constrained binary symmetric channel capacity," *Ann. Appl. Probab.*, vol. 19, no. 3, pp. 1063–1091, 2009.
- [20] D. Shaviv, A. Ozgur, and H. Permuter, "Can feedback increase the capacity of the energy harvesting channel?" in *Proc. IEEE Information Theory Workshop (ITW)*, 2015, available at [arxiv.org:1506.02026](https://arxiv.org/abs/1506.02026).
- [21] Y. Li and G. Han, "Asymptotics of input-constrained erasure channel capacity," May 2016, submitted to *IEEE Trans. Inf. Theory*. Available at [arxiv.org/abs/1605.02175](https://arxiv.org/abs/1605.02175).

- [22] J. P. M. Schalkwijk and T. Kailath, "Coding scheme for additive noise channels with feedback I: No bandwidth constraint," *IEEE Trans. Inf. Theory*, vol. 12, pp. 172–182, 1966.
- [23] T. P. Coleman, "A stochastic control viewpoint on posterior matching feedback communication schemes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, June 2009, pp. 1520–1524.
- [24] C. T. Li and A. E. Gamal, "An efficient feedback coding scheme with low error probability for discrete memoryless channels," *IEEE Trans. Inf. Theory*, vol. 61, no. 6, pp. 2953–2963, June 2015.
- [25] O. Shayevitz and M. Feder, "A simple proof for the optimality of randomized posterior matching," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3410–3418, June 2016.
- [26] O. Sabag, H. Permuter, and H. Pfister, "A single-letter upper bound on the feedback capacity of unifilar finite-state channels," *IEEE Trans. on Inf. Theory*, vol. PP, no. 99, pp. 1–1, Dec. 2016.
- [27] T. M. Cover, "Enumerative source encoding," *IEEE Trans. Inf. Theory*, vol. 19, pp. 73–77, 1973.
- [28] A. Thangaraj, "Dual capacity upper bounds for noisy runlength constrained channels," in *Proc. IEEE Information Theory Workshop (ITW), 2016 IEEE*, 2016, full version: [arxiv.org/abs/1609.00189](https://arxiv.org/abs/1609.00189).
- [29] O. Sabag, H. Permuter, and N. Kashyap, "The feedback capacity of the binary symmetric channel with a no-consecutive-ones input constraint," in *Proc. Allerton Conference Communication, Control, and Computing*, 2015.
- [30] A. Arapostathis, V. S. Borkar, E. Fernandez-Gaucherand, M. K. Ghosh, and S. Marcus, "Discrete time controlled Markov processes with average cost criterion - a survey," *SIAM Journal of Control and Optimization*, vol. 31, no. 2, pp. 282–344, 1993.
- [31] A. Anastasopoulos, "A sequential transmission scheme for unifilar finite-state channels with feedback based on posterior matching," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, July 2012, pp. 2914–2918.
- [32] J. Wu and A. Anastasopoulos, "Zero-rate achievability of posterior matching schemes for channels with memory," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, June 2016, pp. 2256–2260.